

UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH

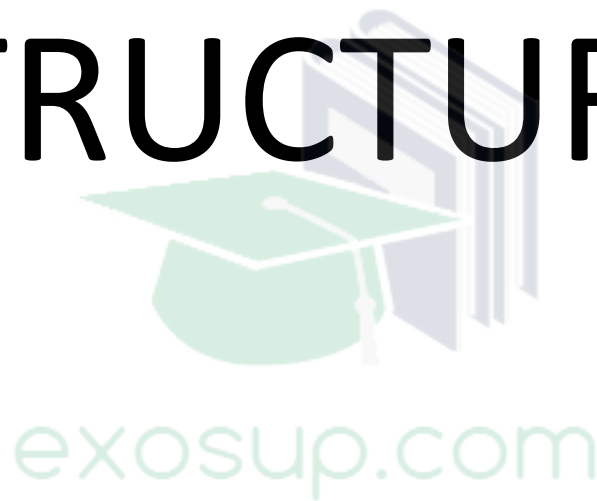
SMA-SMI

FACULTÉ DES SCIENCES DHAR EL MEHRAZ

DÉPARTEMENT DE MATHÉMATIQUES

FES

# STRUCTURES



Pr MOMMED ZENNAYI

# TABLE DES MATIÈRES

|                                                 |        |
|-------------------------------------------------|--------|
| 1-Lois de composition internes.....             | 1      |
| 1-1 Définitions et notations.....               | 1      |
| 1-2 Exemples.....                               | 5      |
| 1-3 Propriétés.....                             | 9      |
| <br>2-Groupe.....                               | <br>33 |
| 2-1 Généralités.....                            | 33     |
| 2-2 Sous-groupes.....                           | 37     |
| 2-3 Classes modulo un sous-groupe.....          | 43     |
| 2-4 Sous-groupes engendrés.....                 | 54     |
| 2-5 Groupes monogènes et groupes cycliques..... | 62     |
| <br>3-Groupe symétrique.....                    | <br>66 |
| 3-1 Généralités.....                            | 66     |
| 3-2 Cycle.....                                  | 71     |
| 3-3 Décomposition d'une permutation.....        | 77     |
| 3-4 Signature d'une permutation.....            | 84     |

|                                          |     |
|------------------------------------------|-----|
| 4-Anneaux et corps.....                  | 90  |
| 4-1 Généralités.....                     | 90  |
| 4-2 Règles de calcul et propriétés.....  | 91  |
| 4-3 Sous-anneaux et sous-corps.....      | 95  |
| 4-4 Fractions et corps de fractions..... | 98  |
| 4-5 Idéaux.....                          | 109 |
| 4-6 Anneaux quotients.....               | 116 |
| 4-7 Caractéristique.....                 | 121 |

## STRUCTURES

### 1 - Lois de composition internes :

#### 1-1- Définitions et notations :

$E$  étant un ensemble quelconque .

- 1) On appelle loi de composition interne dans  $E$  ou loi dans  $E$  toute application de  $E \times E$  vers  $E$ .
- 2) Si  $f$  est une loi de composition interne dans  $E$  alors :  
 $\forall (x, y) \in E \times E : f((x, y))$  est noté  $x f y$ .
- 3) Les lois de composition internes dans  $E$  sont en général notées par les symboles :  
 $\star, T, \perp, \div, \times, \bullet, \dots$
- 4) Si  $\star$  est une loi de composition interne dans  $E$ , on dit que  $E$  est muni d'une de la loi de composition interne  $\star$  ou  $(E, \star)$  est un ensemble muni de la loi de composition interne  $\star$ .

**Par la suite  $(E, \star)$  est un ensemble quelconque muni d'une de la loi de composition interne  $\star$ .**

- 5) Si la loi de composition interne dans  $E$  est notée  $+$  on dit que la loi de  $E$  est additive ou  $E$  est additif.
- 6) Si la loi de composition interne dans  $E$  est notée  $\times, \bullet$ , on dit que la loi de  $E$  est multiplicative ou  $E$  est multiplicatif.
- 7) Si  $a_1, a_2, \dots, a_n$  sont des éléments quelconques de  $E$ , on définit par récurrence sur  $n \in \mathbb{N}^*$  l'élément de  $E$  noté  $\star_{k=1}^n a_k$  par :

$$\begin{cases} \star_{k=1}^1 a_k = a_1 & \text{si } n = 1 \\ \star_{k=1}^n a_k = (\star_{k=1}^{n-1} a_k) \star a_n & \text{si } n \geq 2 \end{cases}.$$

- 8) Si la loi  $\star$  est multiplicative alors :

- $\forall a_1, a_2, \dots, a_n \in E : \star_{k=1}^n a_k$  est noté  $\prod_{k=1}^n a_k$  (c'est à dire :  $\prod_{k=1}^n a_k = \star_{k=1}^n a_k$ ).
- $\forall a \in E$  et  $\forall n \in \mathbb{N}^* : a^n = \prod_{k=1}^n a_k$  avec :  $a_1 = a_2 = \dots = a_n = a$ .

**Remarque 1-1-1 :**

Pour tout élément  $a$  de  $E$  et pour tout entier naturel non nul  $n$  on a :  $a^{n+1} = a^n a$ .  
C'est à dire :  $\forall a \in E$  et  $\forall n \in \mathbb{N}^* : a^{n+1} = a^n a$ .

**En effet :**

Soit  $a$  un élément de  $E$  et  $n$  un entier naturel non nul.

Pour tout entier naturel  $k = 1, 2, \dots, n+1$ , posons  $a_k = a$ .

$$a^{n+1} = \prod_{k=1}^{n+1} a_k = \left( \prod_{k=1}^n a_k \right) a_{n+1} = a^n a.$$

9) Si la loi  $\star$  est additive alors :

- $\forall a_1, a_2, \dots, a_n \in E : +_{k=1}^n a_k$  est noté  $\sum_{k=1}^n a_k$  (c'est à dire :  $\sum_{k=1}^n a_k = +_{k=1}^n a_k$ ).
- $\forall a \in E$  et  $\forall n \in \mathbb{N}^* : na = \sum_{k=1}^n a_k$  avec :  $a_1 = a_2 = \dots = a_n = a$ .

**Remarque 1-1-2 :**

Pour tout élément  $a$  de  $E$  et pour tout entier naturel non nul  $n$  on a :

$$(n+1)a = na + a.$$

C'est à dire :  $\forall a \in E$  et  $\forall n \in \mathbb{N}^* : (n+1)a = na + a$ .

**En effet :**

Soit  $a$  un élément de  $E$  et  $n$  un entier naturel non nul.

Pour tout entier naturel  $k = 1, 2, \dots, n+1$ , posons  $a_k = a$ .

$$(n+1)a = \sum_{k=1}^{n+1} a_k = \sum_{k=1}^n a_k + a_{n+1} = na + a.$$

10) On dit qu'une partie  $A$  de  $E$  est stable pour la loi de  $E$  ou  $A$  est une partie stable de  $E$  si on a :  $\forall x, y \in A : x \star y \in A$ .

11) Si  $A$  est une partie de  $E$  stable pour la loi de  $E$  alors la restriction de la loi  $\star$  à  $A \times A$  qui est aussi une loi de composition interne dans  $A$  est appelée la restriction de la loi de composition interne (ou la restriction de la loi)  $\star$  dans  $A$ .

12) Si  $A$  est une partie de  $E$  stable pour la loi de  $E$ , la restriction de la loi  $\star$  à  $A$  est notée aussi  $\star$  (notée de la même façon que la notation de la loi de  $E$ ).

13) Soient  $x$  et  $y$  deux éléments quelconques de  $E$ .

On dit que  $x$  commute avec  $y$  (pour la loi  $\star$ ) ou  $x$  et  $y$  commutent (pour la loi  $\star$ ) si on a :  $x \star y = y \star x$ .

14) Si tous les éléments de  $E$  commutent (pour la loi  $\star$ ) on dit que la loi  $\star$  est commutative ou abélien. C'est à dire :

$$[\text{la loi } \star \text{ est commutative}] \Leftrightarrow [\text{la loi } \star \text{ est abélien}] \Leftrightarrow [\forall x, y \in E : x \star y = y \star x].$$

15) On dit que la loi  $\star$  est associative si on a :  $\forall x, y, z \in E : (x \star y) \star z = x \star (y \star z)$ .

**Dans ce cas** :  $\forall x, y, z \in E : (x \star y) \star z = x \star (y \star z)$  est noté aussi :  $x \star y \star z$

C'est à dire :  $\forall x, y, z \in E : (x \star y) \star z = x \star (y \star z) = x \star y \star z$ .

16) Si  $T$  est une autre loi de composition interne dans  $E$  on dit que la loi  $\star$  est distributive par rapport à  $T$  si on a :

$$\forall x, y, z \in E : \begin{cases} x \star (yTz) = (x \star y)T(x \star z) \\ (yTz) \star x = (y \star x)T(z \star x) \end{cases}.$$

17) On dit qu'un élément  $e \in E$  est l'élément neutre de  $E$  si on a :

$$\forall x \in E : x \star e = e \star x = x.$$

**Remarque 1-1-3 :**

Si  $E$  admet un élément neutre pour la loi  $\star$ , cet élément neutre est unique

**En effet :**

Soient  $e$  et  $e'$  deux éléments neutres de  $E$  pour la loi de composition interne  $\star$ .

$$\begin{cases} \text{Puisque } e' \text{ est un élément neutre de } E \text{ pour la loi } \star \text{ alors : } e \star e' = e \\ \text{Puisque } e \text{ est un élément neutre de } E \text{ pour la loi } \star \text{ alors : } e \star e' = e' \end{cases}.$$

Donc :  $e = e \star e' = e'$  D'où l'unicité de l'élément neutre.

18) Si la loi de  $E$  est multiplicative et si  $E$  admet un élément neutre  $e$  pour la loi de  $E$  alors pour tout élément  $a$  de  $E$ , on note :  $a^0 = e$ .

19) Si la loi de  $E$  est additive et si  $E$  admet un élément neutre pour la loi de  $E$  alors :

- l'élément neutre de  $E$  est appelé le zéro de  $E$  ou zéro et noté  $0_E$  ou  $0$ .
- $\forall a \in E$  : on note :  $0a = 0_E$ .

20) Soient  $x$  et  $x'$  deux éléments quelconques de  $E$ .

Si  $E$  admet un élément neutre  $e$  pour la loi de  $E$  et si on a :  $x \star x' = x' \star x = e$  on dit que  $x$  est symétrisable pour la loi de  $E$  et que  $x'$  est son symétrique.

**Remarque 1-1-4 :**

Dans le cas où la loi  $\star$  de  $E$  est associative et  $E$  admet un élément neutre, si un élément  $x$  est symétrisable alors son symétrique est unique.

**En effet :**

Supposons que loi  $\star$  de  $E$  est associative,  $E$  admet un élément neutre  $e$  et  $x$  est un élément symétrisable de  $E$  pour la loi  $\star$ .

Soient  $x'$  et  $x''$  deux symétriques de  $x$ .

$$x' = e \star x' = (x'' \star x) \star x' = x'' \star (x \star x') = x'' \star e = x''.$$

D'où l'unicité du symétrique de  $x$ .

21) Si la loi de  $E$  est multiplicative et si  $E$  admet un élément neutre alors :

- Les éléments symétrisables pour la loi de  $E$  sont appelés les éléments inversibles de  $E$  ou les éléments inversibles.

- Si  $x$  est un élément inversible de  $E$ , son symétrique est appelé l'inverse de  $x$ .
- Si  $x$  est un élément inversible de  $E$  et si  $x'$  est l'inverse de  $x$  alors pour tout entier relatif strictement négatif  $n$  on note par  $x^n$  l'élément  $x^n = (x')^{-n}$ .  
C'est à dire si  $x'$  est l'inverse de  $x$  alors :  $\forall n \in \mathbb{Z}^{*-} : x^n = (x')^{-n}$ .

22) Si la loi de  $E$  est additive et si  $E$  admet un zéro alors :

- Si  $x$  est un élément de  $E$  et si  $x$  admet un symétrique  $x'$  alors  $x'$  est appelé l'opposé de  $x$  et noté  $-x$ .
- Si  $x$  est un élément de  $E$  qui admet un et opposé alors pour tout entier relatif strictement négatif  $n$  on note par  $nx$  l'élément  $nx = (-n)(-x)$ .  
C'est à dire si  $x$  admet un opposé alors :  $\forall n \in \mathbb{Z}^{*-} : nx = (-n)(-x)$ .
- Si  $x, y \in E$  sont deux éléments quelconques de  $E$  et si  $y$  admet un opposé alors  $x + (-y)$  est noté aussi  $x - y$  (Dans ce cas on a donc :  $x - y = x + (-y)$ ).

23) On dit qu'un élément  $a$  de  $E$  est absorbant pour la loi  $\star$  de  $E$  si on a :

$$\forall x \in E : x \star a = a \star x = a.$$

### Remarque 1-1-5 :

Si  $E$  admet un élément absorbant pour la loi  $\star$ , cet élément absorbant est unique

### En effet :

Soient  $a$  et  $a'$  deux éléments absorbants de  $E$  pour la loi de composition interne  $\star$ .

$$\begin{cases} \text{Puisque } a \text{ est un élément absorbant de } E \text{ pour la loi } \star \text{ alors : } a \star a' = a \\ \text{Puisque } a' \text{ est un élément absorbant de } E \text{ pour la loi } \star \text{ alors : } a \star a' = a' \end{cases}$$

Donc :  $a = a \star a' = a'$  D'où l'unicité de l'élément absorbant .

24) On dit qu'un élément  $a$  de  $E$  est régulier pour la loi de  $E$  si on a :

$$\forall x, y \in E : \begin{cases} x \star a = y \star a \Rightarrow x = y \\ a \star x = a \star y \Rightarrow x = y \end{cases}$$

25) Si  $(F, T)$  est un autre ensemble muni d'une loi de composition interne  $T$  et si  $f$  est une application de  $E$  vers  $F$  on dit que  $f$  est un homomorphisme de  $(E, \star)$  vers  $(F, T)$  ou  $f$  est un homomorphisme de  $E$  vers  $F$  si la propriété suivante est vérifiée :  $\forall x, y \in E : f(x \star y) = f(x)Tf(y)$ .

### En particulier :

- Si  $F$  admet un élément neutre  $\varepsilon$  pour la loi  $T$  alors l'ensemble suivant :  
 $\{x \in E \text{ tq : } f(x) = \varepsilon\}$  est appelé le noyau de  $f$  ou le  $\ker$  de  $f$  et noté  $\ker f$ .
- Si  $f$  est bijective on dit que  $f$  est un isomorphisme de  $(E, \star)$  vers  $(F, T)$  ou  $f$  est un isomorphisme de  $E$  vers  $F$

26) Si  $(F, T)$  est un autre ensemble muni d'une loi de composition interne  $T$  et s'il existe un isomorphisme de  $(E, \star)$  vers  $(F, T)$  on dit que  $(E, \star)$  est isomorphe à  $(F, T)$  ou  $E$  est isomorphe à  $F$  ou  $(E, \star)$  et  $(F, T)$  sont isomorphes ou  $E$  et  $F$  sont isomorphes et on note  $(E, \star) \simeq (F, T)$  ou  $E \simeq F$ .

## 1-2-Exemples :

1)  $\mathbb{N}$ ,  $\mathbb{N}^*$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$  munis de l'addition et de la multiplication.

- L'addition et la multiplication sont commutatives et associatives.
- La multiplication distributive par rapport à l'addition.
- $\mathbb{N}^*$  n'admet pas de zéro pour l'addition.
- 0 est le zéro pour les ensembles  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ .
- 1 est l'élément neutre pour la multiplication.
- 0 est le seul élément qui admet un opposé dans  $\mathbb{N}$ .
- Dans les ensembles  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$  tout élément admet un opposé.
- 1 est le seul élément inversible dans les ensembles  $\mathbb{N}$  et  $\mathbb{N}^*$ .
- 1 et  $-1$  sont les seuls éléments inversibles dans l'ensemble  $\mathbb{Z}$ .
- Tous les éléments non nuls sont inversibles dans les ensembles  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ .
- Pour la multiplication 0 est un élément absorbant pour les ensembles  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ .
- Tous les éléments sont réguliers pour l'addition.
- Tous les éléments non nuls sont réguliers pour la multiplication.
- $\{1, -1\}$  est une partie stable de  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{Q}^*$ ,  $\mathbb{R}$ ,  $\mathbb{R}^*$ ,  $\mathbb{C}$  et  $\mathbb{C}^*$  pour la multiplication.

2)  $\mathcal{P}(E)$  muni des lois de composition internes :  $\cup$ ,  $\cap$ , et  $\Delta$ .

- $\cup$ ,  $\cap$ , et  $\Delta$  sont commutatives et associatives.
- $\cup$  est distributive par rapport à  $\cup$  et par rapport à  $\cap$ .
- $\cap$  est distributive par rapport à  $\cap$ , par rapport à  $\cup$  et par rapport à  $\Delta$ .
- $\emptyset$  est l'élément neutre de  $\mathcal{P}(E)$  pour la loi  $\cup$ .
- $\emptyset$  est le seul élément symétrisable de  $\mathcal{P}(E)$  pour la loi  $\cup$ .
- $E$  est l'élément absorbant de  $\mathcal{P}(E)$  pour la loi  $\cup$ .
- $E$  est le seul élément régulier de  $\mathcal{P}(E)$  pour la loi  $\cup$ .
- $E$  est l'élément neutre de  $\mathcal{P}(E)$  pour la loi  $\cap$ .
- $E$  est le seul élément symétrisable de  $\mathcal{P}(E)$  pour la loi  $\cap$ .
- $\emptyset$  est l'élément absorbant de  $\mathcal{P}(E)$  pour la loi  $\cap$ .
- $\emptyset$  est le seul élément régulier de  $\mathcal{P}(E)$  pour la loi  $\cap$ .
- $\emptyset$  est l'élément neutre de  $\mathcal{P}(E)$  pour la loi  $\Delta$ .
- Tous les éléments de  $\mathcal{P}(E)$  sont symétrisables pour la loi  $\Delta$ .
- $\forall A \in \mathcal{P}(E)$  :  $A$  est le symétrique de  $A$  lui même pour la loi  $\Delta$ .
- $\mathcal{P}(E)$  n'admet pas d'élément absorbant pour la loi  $\Delta$ .
- Tous les éléments de  $\mathcal{P}(E)$  sont réguliers pour la loi  $\Delta$ .

3) Soit  $(E, *)$  un ensemble muni d'une loi de composition interne  $*$ .

On définit dans  $\mathcal{P}(E)$  la loi de composition interne suivante notée aussi  $*$  :

$$\forall X, Y \in \mathcal{P}(E) : X * Y = \{x * y \text{ tq : } x \in X \text{ et } y \in Y\}$$

Cette loi de composition interne  $*$  dans  $\mathcal{P}(E)$  est appelée la loi de composition de  $E$  induite à  $\mathcal{P}(E)$ .

$$\forall a \in E \text{ et } \forall X \in \mathcal{P}(E) :$$

$$\{a\} * X \text{ est noté } a * X \text{ et } X * \{a\} \text{ est noté } X * a.$$

$$\text{C'est à dire : } \{a\} * X = a * X \text{ et } X * \{a\} = X * a.$$

- La loi  $*$  dans  $E$  est commutative si et seulement si la induite à  $\mathcal{P}(E)$  est commutative.



- La loi  $\star$  dans  $E$  est associative si et seulement si la induite à  $\mathcal{P}(E)$  est associative.
- Si  $e \in E$  est un élément de  $E$  alors  $e$  est un élément neutre de  $E$  si et seulement si  $\{e\}$  est un élément neutre de  $\mathcal{P}(E)$  pour la induite à  $\mathcal{P}(E)$ .
- $\emptyset$  est l'élément absorbant de  $\mathcal{P}(E)$  pour la induite.

4) Soient  $(E_1, *_1)$  et  $(E_2, *_2)$  deux ensembles munis des lois de composition internes  $*_1$  et  $*_2$ .

On définit dans l'ensemble :  $E_1 \times E_2$  la loi de composition interne suivante :

$$\forall x = (x_1, x_2) \in E_1 \times E_2 \text{ et } \forall y = (y_1, y_2) \in E_1 \times E_2 :$$

$$x * y = (x_1 *_1 y_1, x_2 *_2 y_2)$$

- La loi  $\star$  est commutative si et seulement si  $*_1$  et  $*_2$  sont commutatives.
- La loi  $\star$  est associative si et seulement si  $*_1$  et  $*_2$  sont associatives.
- Un élément  $e = (e_1, e_2) \in E_1 \times E_2$  est un élément neutre de  $E_1 \times E_2$  pour la loi  $\star$  si et seulement si  $e_1$  est un élément neutre de  $E_1$  pour la loi  $*_1$  et  $e_2$  est un élément neutre de  $E_2$  pour la loi  $*_2$ .
- Soient  $e_1$  un élément neutre de  $E_1$  pour la loi  $*_1$ ,  $e_2$  un élément neutre de  $E_2$  pour la loi  $*_2$  et  $x = (x_1, x_2) \in E_1 \times E_2$  un élément quelconque de  $E_1 \times E_2$ . Pour que  $x = (x_1, x_2)$  soit symétrisable il faut et suffit que  $x_1$  et  $x_2$  sont symétrisables.

**Dans ce cas :**

Si  $x'_1$  et  $x'_2$  sont les symétriques de  $x_1$  et  $x_2$  alors  $x' = (x'_1, x'_2)$  est le symétrique de  $x = (x_1, x_2)$ .

- **Dans le cas additif :**  $-x = -(x_1, x_2) = (-x_1, -x_2)$ .
- **Dans le cas multiplicatif :**  $x^{-1} = (x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$ .
- Un élément  $a = (a_1, a_2) \in E_1 \times E_2$  est régulier pour la loi  $\star$  si et seulement si  $a_1$  et  $a_2$  sont réguliers pour les lois  $*_1$  et  $*_2$ .
- Si les lois de  $E_1$  et  $E_2$  sont multiplicatives et si  $a = (a_1, a_2) \in E_1 \times E_2$  est un élément quelconque de  $E_1 \times E_2$ . alors :
  - $\forall n \in \mathbb{N}^* : a^n = (a_1, a_2)^n = (a_1^n, a_2^n)$
  - $\forall n \in \mathbb{N} : a^n = (a_1, a_2)^n = (a_1^n, a_2^n)$  si  $E_1$  et  $E_2$  possèdent des éléments neutres.
  - $\forall n \in \mathbb{Z} : a^n = (a_1, a_2)^n = (a_1^n, a_2^n)$  si  $E_1$  et  $E_2$  possèdent des éléments neutres et si  $a_1$  et  $a_2$  sont inversibles.
- Si les lois de  $E_1$  et  $E_2$  sont additives et si  $a = (a_1, a_2) \in E_1 \times E_2$  est un élément quelconque de  $E_1 \times E_2$ . alors :
  - $\forall n \in \mathbb{N}^* : na = n(a_1, a_2) = (na_1, na_2)$
  - $\forall n \in \mathbb{N} : na = n(a_1, a_2) = (na_1, na_2)$  si  $E_1$  et  $E_2$  possèdent des zéros.
  - $\forall n \in \mathbb{Z} : na = n(a_1, a_2) = (na_1, na_2)$  si  $E_1$  et  $E_2$  possèdent des zéros et si  $a_1$  et  $a_2$  possèdent des opposés.

5) Soient  $I$  un ensemble non vide et  $((E_i, *_i))_{i \in I}$  une famille d'ensembles muni chacun d'une loi de composition interne.

On définit dans l'ensemble :  $\prod_{i \in I} E_i$  la loi de composition interne suivante :

$$\forall x = (x_i)_{i \in I} \in \prod_{i \in I} E_i \text{ et } \forall y = (y_i)_{i \in I} \in \prod_{i \in I} E_i :$$

$$x * y = (x_i)_{i \in I} *_i (y_i)_{i \in I} = (x_i *_i y_i)_{i \in I}.$$

- La loi  $\star$  est commutative si seulement si :  $\forall i \in I : \star_i$  est commutative .
- La loi  $\star$  est associative si seulement si :  $\forall i \in I : \star_i$  est associatives .
- Un élément  $e = (e_i)_{i \in I} \in \prod_{i \in I} E_i$  est un élément neutre de  $\prod_{i \in I} E_i$  pour la loi  $\star$  si seulement si :  $\forall i \in I : e_i$  est un élément neutre de  $E_i$  pour la loi  $\star_i$  .
- Soient  $e = (e_i)_{i \in I} \in \prod_{i \in I} E_i$  un élément neutre de  $\prod_{i \in I} E_i$  pour la loi  $\star$  et  $x = (x_i)_{i \in I} \in \prod_{i \in I} E_i$  un élément quelconque de  $\prod_{i \in I} E_i$  .  
Pour que  $x = (x_i)_{i \in I}$  soit symétrisable il faut et suffit que :  
 $\forall i \in I : x_i$  est symétrisables .

**Dans ce cas :**

Si on a :  $\forall i \in I : x'_i$  est le symétrique de  $x_i$  alors  $x' = (x'_i)_{i \in I}$  est le symétrique de  $x = (x_i)_{i \in I}$  .

- **Dans le cas additif** :  $-x = -(x_i)_{i \in I} = (-x_i)_{i \in I}$  .

- **Dans le cas multiplicatif** :  $x^{-1} = (x_i)^{-1}_{i \in I} = (x_i^{-1})_{i \in I}$  .

- Un élément  $a = (a_i)_{i \in I} \in \prod_{i \in I} E_i$  est régulier pour la loi  $\star$  si seulement si :  
 $\forall i \in I : a_i$  est régulier pour la loi  $\star_i$  .
- Si on a :  $\forall i \in I : E_i$  est multiplicative et si  $a = (a_i)_{i \in I} \in \prod_{i \in I} E_i$  est un élément quelconque de  $\prod_{i \in I} E_i$  alors :  
  - $\forall n \in \mathbb{N}^* : a^n = (a_i)^n_{i \in I} = (a_i^n)_{i \in I}$
  - $\forall n \in \mathbb{N} : a^n = (a_i)^n_{i \in I} = (a_i^n)_{i \in I}$  si :  $\forall i \in I : E_i$  possède un élément neutre.
  - $\forall n \in \mathbb{Z} : a^n = (a_i)^n_{i \in I} = (a_i^n)_{i \in I}$  si :  $\forall i \in I : E_i$  possède un élément neutre et si :  $\forall i \in I : a_i$  est inversible.
- Si on a :  $\forall i \in I : E_i$  est additive et si  $a = (a_i)_{i \in I} \in \prod_{i \in I} E_i$  est un élément quelconque de  $\prod_{i \in I} E_i$  . alors :  
  - $\forall n \in \mathbb{N}^* : na = n(a_i)_{i \in I} = (na_i)_{i \in I}$
  - $\forall n \in \mathbb{N} : na = n(a_i)_{i \in I} = (na_i)_{i \in I}$  si :  $\forall i \in I : E_i$  possède un zéro.
  - $\forall n \in \mathbb{Z} : na = n(a_i)_{i \in I} = (na_i)_{i \in I}$  si :  $\forall i \in I : E_i$  possède un zéro et si :  $\forall i \in I : E_i$  possède  $a_i$  possède un opposé.

6) Soient  $E$  un ensemble quelcoque non vide et  $(F, \star)$  un ensemble quelcoque non vide muni d'une loi de composition interne  $\star$ .

- $\forall u, v \in F^E : u \star v : E \rightarrow F$   
$$x \mapsto (u \star v)(x) = u(x) \star v(x).$$

**En effet :**

$$\forall u, v \in F^E : u \star v = (u(x))_{x \in E} \star (v(x))_{x \in E} = (u(x)_x \star v(x))_{x \in E}$$

Donc  $u \star v$  est l'application de  $E$  vers  $F$  définie par :

$$u \star v : E \rightarrow F$$

$$x \mapsto (u \star v)(x) = u(x) \star v(x).$$

- La loi de composition interne  $\star$  dans  $F^E$  est commutative si seulement si la loi de composition interne  $\star$  dans  $F$  est commutative .

$$\text{Car : } F^E = \prod_{x \in E} F_x \quad tq : \forall x \in E : F_x = F$$

- La loi de composition interne  $\star$  dans  $F^E$  est associative si seulement si la loi de composition interne  $\star$  dans  $F$  est associative.

$$\text{Car : } F^E = \prod_{x \in E} F_x \quad tq : \forall x \in E : F_x = F.$$

- Si  $e \in F$  est un élément quelconque de  $F$  alors  $e$  est l'élément neutre de  $F$  si seulement si l'application suivante :

$$\varepsilon : E \rightarrow F$$

$$x \mapsto \varepsilon(x) = e$$

est l'élément neutre de  $F^E$ .

**En effet :**

$$\forall x \in E : \text{posons } F_x = F \text{ et } e_x = e .$$

$$\text{Alors : } \forall x \in E : e_x = e \text{ est l'élément neutre de } F_x = F \text{ et } F^E = \prod_{x \in E} F_x.$$

$$\text{Donc : } \varepsilon = (\varepsilon(x))_{x \in E} = (e_x)_{x \in E} \text{ est l'élément neutre de } F^E = \prod_{x \in E} F_x.$$

- Si  $e \in F$  est l'élément neutre de  $F$  et si  $u \in F^E$  est un élément quelconque de  $F^E$  alors  $u$  est symétrisable si et seulement si :  $\forall x \in E : u(x)$  est symétrisable.

Et de ce cas l'application suivante :

$$u' : E \rightarrow F$$

$$x \mapsto u'(x) = u(x)' \quad (\text{tel que : } \forall x \in E : u(x)' \text{ est le symétrique de } u(x))$$

est le symétrique de  $u$  dans  $F^E$ .

**En effet :**

$$\forall x \in E : \text{posons } F_x = F$$

$$u \text{ est symétrisable dans } F^E \Leftrightarrow (u(x))_{x \in E} \text{ est symétrisable dans } \prod_{x \in E} F_x = F^E$$

$$\Leftrightarrow \forall x \in E : u(x) \text{ est symétrisable dans } F_x = F.$$

**Dans ce cas :**

$$\text{Si } \begin{cases} u' \text{ est le symétrique de } u \text{ dans } F^E \\ \forall x \in E : u(x)' \text{ est le symétrique de } u(x) \text{ dans } F = F_x \end{cases} \quad \text{alors :}$$

$$u' = ((u(x))'_{x \in E}) = (u(x)')_{x \in E}$$

Donc : l'application  $u'$  est définie pare :  $u' : E \rightarrow F$

$$x \mapsto u'(x) = u(x)'$$

- **Dans le cas additif :**  $\forall u \in F^E$  et  $\forall x \in E : (-u)x = -u(x)$

- **Dans le cas multiplicatif :**  $\forall u \in F^E$  et  $\forall x \in E : u^{-1}(x) = u(x)^{-1}$

- Si  $F$  est multiplicatif et si  $u \in F^E$  est un élément quelconque de  $F^E$  alors :

$$- \forall x \in E \text{ et } \forall n \in \mathbb{N}^* : u^n(x) = u(x)^n$$

$$- \forall x \in E \text{ et } \forall n \in \mathbb{N} : u^n(x) = u(x)^n$$

$$- \forall x \in E \text{ et } \forall n \in \mathbb{Z} : u^n(x) = u(x)^n$$

si :  $F$  possède un élément neutre.

si :  $F$  possède un élément neutre

et si :  $\forall x \in E : u(x)$  est inversible.

- Si  $F$  est additif et si  $u \in F^E$  est un élément quelconque de  $F^E$  alors :
  - $\forall x \in E$  et  $\forall n \in \mathbb{N}^* : (nu)(x) = nu(x)$
  - $\forall x \in E$  et  $\forall n \in \mathbb{N} : (nu)(x) = nu(x)$  si :  $F$  possède un zéro.
  - $\forall x \in E$  et  $\forall n \in \mathbb{Z} : (nu)(x) = nu(x)$  si :  $F$  possède un zéro et si :  $\forall x \in E : u(x)$  possède un opposé.
- Un élément  $u \in F^E$  est régulier si seulement si :  $\forall x \in E : u(x)$  est régulier.

7) Soit  $E$  un ensemble. La composition des applications de  $E$  vers  $E$  est une loi de composition interne dans l'ensemble  $E^E$  (c'est à dire  $\circ$  une loi de composition interne dans l'ensemble  $E^E$ ).

- $id_E$  est l'élément neutre de  $E^E$  pour la loi  $\circ$ .
- Un élément  $f$  de  $E^E$  est symétrisable pour la loi  $\circ$  si seulement si  $f$  est une permutation de  $E$  et dans ce cas, la réciproque  $f^{-1}$  de  $f$  est le symétrique de  $f$ .
- L'ensemble des applications injectives de  $E$  vers  $E$ , l'ensemble des applications surjectives de  $E$  vers  $E$  et l'ensemble des permutations de  $E$  sont des parties stables de  $E$  pour la loi  $\circ$ . Par la suite on a donc :  
 $\circ$  est une loi de compositions interne dans l'ensemble des applications injectives de  $E$  vers  $E$ , dans l'ensemble des applications surjectives de  $E$  vers  $E$  et dans l'ensemble des permutations de  $E$ .

### 1-3-Propriétés :

#### Proposition 1-3-1 :

Soient  $(E, .)$  un ensemble muni d'une loi de composition interne associative, notée multiplicativement et  $x, y$  deux éléments quelconques de  $E$ .

Les cinq propriétés suivantes sont vérifiées.

- 1)  $\forall n, m \in \mathbb{N}^* : x^n x^m = x^{n+m}$ .
- 2)  $\forall n, m \in \mathbb{N}^* : (x^n)^m = x^{nm}$ .
- 3) si  $x$  et  $y$  commutent alors pour tout entier naturel non nul  $n$ , l'élément  $x$  commute avec  $y^n$ . C'est à dire :  $xy = yx \Rightarrow \forall n \in \mathbb{N}^* : xy^n = y^n x$ .
- 4) si  $x$  et  $y$  commutent alors :  $\forall n, m \in \mathbb{N}^* : x^n$  et  $y^m$  commutent.  
**En particulier** :  $\forall n, m \in \mathbb{N}^* : x^n$  et  $x^m$  commutent.
- 5) si  $x$  et  $y$  commutent alors :  $\forall n \in \mathbb{N}^* : (xy)^n = x^n y^n$ .

#### Démonstration :

- 1) Montrons par récurrence sur  $m \in \mathbb{N}^*$  que pour tout entier naturel non nul  $n$  on a :  
 $x^n x^m = x^{n+m}$ .

- **Pour  $m = 1$  :**

$$\forall n \in \mathbb{N}^* : x^n x^1 = x^n x^1 = x^{n+1} = x^{n+m}.$$

- **Pour  $m - 1$  :**

Supposons que pour tout entier naturel non nul  $n$  on a :  $x^n x^{m-1} = x^{n+(m-1)}$ .

- **Pour  $m$  :**

Montrons qu'alors pour tout entier naturel non nul  $n$  on a :  $x^n x^m = x^{n+m}$ .

Soit  $n$  un entier naturel non nul quelconque.

$$\begin{aligned} x^n x^m &= x^n (x^{m-1} x) = (x^n x^{m-1}) x = (x^{n+(m-1)}) x \text{ (d'après l'hypothèse de récurrence)} \\ &= x^{n+m-1} x = x^{(n+m-1)+1} = x^{n+m-1+1} \\ &= x^{n+m}. \end{aligned}$$

2) Montrons par récurrence sur  $m \in \mathbb{N}^*$  que pour tout entier naturel non nul  $n$  on a :

$$(x^n)^m = x^{nm}.$$

- **Pour  $m = 1$  :**

$$\forall n \in \mathbb{N}^* : (x^n)^m = (x^n)^1 = x^n = x^{n1} = x^{nm}.$$

- **Pour  $m - 1$  :**

Supposons que pour tout entier naturel non nul  $n$  on a :  $(x^n)^{m-1} = x^{n(m-1)}$ .

- **Pour  $m$  :**

Montrons qu'alors pour tout entier naturel non nul  $n$  on a :  $(x^n)^m = x^{nm}$ .

Soit  $n$  un entier naturel non nul quelconque.

$$\begin{aligned} (x^n)^m &= (x^n)^{m-1+1} = (x^n)^{m-1} x^n \\ &= x^{n(m-1)} x^n \text{ (d'après l'hypothèse de récurrence)} \\ &= x^{n(m-1)+n} \text{ (d'après la propriété a)} \\ &= x^{nm-n+n} \\ &= x^{nm}. \end{aligned}$$

3) Supposons que  $x$  et  $y$  commutent.

Montrons par récurrence que pour tout entier naturel non nul  $n$ ,  $x$  commute avec  $y^n$ .

- **Pour  $n = 1$  :**

$$xy^n = xy^1 = xy = yx = y^1x = y^nx. \text{ Donc } x \text{ commute avec } y^n.$$

- **Pour  $n - 1$  :**

Supposons que  $x$  commute avec  $y^{n-1}$ .

- **Pour  $n$  :**

Montrons qu'alors  $x$  commute avec  $y^n$ .

$$\begin{aligned} xy^n &= x(y^{n-1}y) = (xy^{n-1})y = (y^{n-1}x)y \text{ (d'après l'hypothèse de récurrence)} \\ &= y^{n-1}(xy) = y^{n-1}(yx) = (y^{n-1}y)x \\ &= y^n x. \end{aligned}$$

Donc  $x$  commute avec  $y^n$ .

4) Supposons que  $x$  et  $y$  commutent.

$\forall n, m \in \mathbb{N}^* :$

Puisque  $x$  et  $y$  commutent, alors (d'après la propriété c))  $x$  commute avec  $y^m$ .

Puisque  $y^m$  et  $x$  commutent, alors (d'après la propriété c))  $y^m$  commute avec  $x^n$ .

Donc  $x^n$  et  $y^m$  commutent.

**En particulier :**  $\forall n, m \in \mathbb{N}^* : x^n$  et  $x^m$  commutent (car  $x$  commute avec  $x$ ).

5) Supposons que  $x$  et  $y$  commutent.

Montrons par récurrence sur  $n \in \mathbb{N}^*$  que  $(xy)^n = x^n y^n$ .

- **Pour  $n = 1$  :**

$$(xy)^n = (xy)^1 = xy = x^1 y^1 = x^n y^n.$$

- **Pour  $n - 1$  :**

Supposons que  $(xy)^{n-1} = x^{n-1} y^{n-1}$ .

- **Pour  $n$  :**

Montrons qu'alors  $(xy)^n = x^n y^n$ .

$$\begin{aligned} (xy)^n &= (xy)^{n-1}(xy) = (x^{n-1}y^{n-1})(xy) \text{ (d'après l'hypothèse de récurrence)} \\ &= x^{n-1}(y^{n-1}x)y = x^{n-1}(xy^{n-1})y \text{ (d'après la propriété c)} \\ &= (x^{n-1}x)(y^{n-1}y) \\ &= x^n y^n. \end{aligned}$$

**Proposition 1-3-2 :**

Soient  $(E, +)$  un ensemble muni d'une loi de composition interne associative, notée additivement et  $x, y$  deux éléments quelconques de  $E$ .

Les cinq propriétés suivantes sont vérifiées.

- 1)  $\forall n, m \in \mathbb{N}^* : nx + mx = (n + m)x$ .
- 2)  $\forall n, m \in \mathbb{N}^* : n(mx) = (nm)x$ .
- 3) si  $x$  et  $y$  commutent alors pour tout entier naturel non nul  $n$ , l'élément  $x$  commute avec  $ny$ . C'est à dire :  $x + y = y + x \Rightarrow \forall n \in \mathbb{N}^* : x + ny = ny + x$ .
- 4) si  $x$  et  $y$  commutent alors :  $\forall n, m \in \mathbb{N}^* : nx$  et  $my$  commutent.  
**En particulier** :  $\forall n, m \in \mathbb{N}^* : nx$  et  $mx$  commutent.
- 5) si  $x$  et  $y$  commutent alors :  $\forall n \in \mathbb{N}^* : n(x + y) = nx + ny$ .

**Démonstration :**

- 1) Montrons par récurrence sur  $m \in \mathbb{N}^*$  que pour tout entier naturel non nul  $n$  on a :

$$nx + mx = (n + m)x.$$

- **Pour  $m = 1$  :**

$$\forall n \in \mathbb{N}^* : nx + mx = nx + 1x = (n + 1)x = (n + m)x.$$

- **Pour  $m - 1$  :**

Supposons que pour tout entier naturel non nul  $n$  on a :

$$nx + (m - 1)x = [n + (m - 1)]x.$$

- **Pour  $m$  :**

Montrons qu'alors pour tout entier naturel non nul  $n$  on a :  $nx + mx = (n + m)x$ .

Soit  $n$  un entier naturel non nul quelconque.

$$\begin{aligned} nx + mx &= nx + [(m - 1)x + x] = [nx + (m - 1)x] + x \\ &= (n + m - 1)x + x \text{ (d'après l'hypothèse de récurrence)} \\ &= [(n + m - 1) + 1]x = (n + m - 1 + 1)x \\ &= (n + m)x. \end{aligned}$$

- 2) Montrons par récurrence sur  $m \in \mathbb{N}^*$  que pour tout entier naturel non nul  $n$  on a :

$$n(mx) = (nm)x.$$

- **Pour  $n = 1$  :**

$$\forall m \in \mathbb{N}^* : n(mx) = 1(mx) = mx = (1m)x = (nm)x.$$

- **Pour  $n - 1$  :**

Supposons que pour tout entier naturel non nul  $m$  on a :

$$(n - 1)(mx) = [(n - 1)m]x.$$

- **Pour  $n$  :**

Montrons qu'alors pour tout entier naturel non nul  $m$  on a :  $n(mx) = (nm)x$ .

Soit  $m$  un entier naturel non nul quelconque.

$$\begin{aligned} n(mx) &= (n - 1)(mx) + mx = ((n - 1)m)x + mx \text{ (d'après l'hypothèse de récurrence)} \\ &= [(n - 1)m + m]x \text{ (d'après la propriété a)} \\ &= (nm - m + m)x \\ &= (nm)x. \end{aligned}$$

- 3) Supposons que  $x$  et  $y$  commutent.

Montrons par récurrence que pour tout entier naturel non nul  $n$ ,  $x$  commute avec  $ny$ .

- **Pour  $n = 1$  :**

$$x + ny = x + 1y = x + y = y + x = 1y + x = ny + x. \text{ Donc } x \text{ commute avec } ny.$$

- **Pour  $n - 1$  :**

Supposons que  $x$  commute avec  $(n - 1)y$ .

- **Pour  $n$  :**

Montrons qu'alors  $x$  commute avec  $ny$ .

$$\begin{aligned}x + ny &= x + [(n-1)y + y] = [x + (n-1)y] + y \\&= [(n-1)y + x] + y \text{ (d'après l'hypothèse de récurrence)} \\&= (n-1)y + (x + y) = (n-1)y + (y + x) = [(n-1)y + y] + x \\&= ny + x.\end{aligned}$$

Donc  $x$  commute avec  $ny$ .

4) Supposons que  $x$  et  $y$  commutent.

$\forall n, m \in \mathbb{N}^*$  :

Puisque  $x$  et  $y$  commutent, alors (d'après la propriété c))  $x$  commute avec  $my$ .

Puisque  $my$  et  $x$  commutent, alors (d'après la propriété c))  $my$  commute avec  $nx$ .

Donc  $nx$  et  $my$  commutent.

**En particulier :**  $\forall n, m \in \mathbb{N}^*$  :  $nx$  et  $mx$  commutent (car  $x$  commute avec  $x$ ).

5) Supposons que  $x$  et  $y$  commutent.

Montrons par récurrence sur  $n \in \mathbb{N}^*$  que  $n(x + y) = nx + ny$ .

- **Pour  $n = 1$  :**

$$n(x + y) = 1(x + y) = x + y = 1x + 1y = nx + ny.$$

- **Pour  $n - 1$  :**

Supposons que  $(n-1)(x + y) = (n-1)x + (n-1)y$ .

- **Pour  $n$  :**

Montrons qu'alors  $n(x + y) = nx + ny$ .

$$\begin{aligned}n(x + y) &= (n-1)(x + y) + (x + y) \\&= [(n-1)x + (n-1)y] + (x + y) \text{ (d'après l'hypothèse de récurrence)} \\&= (n-1)x + [(n-1)y + x] + y \\&= (n-1)x + [x + (n-1)y] + y \text{ (d'après la propriété c))} \\&= [(n-1)x + x] + [(n-1)y + y] \\&= nx + ny.\end{aligned}$$

### Proposition 1-3-3 :

Soit  $(E, \star)$  un ensemble muni d'une loi de composition interne associative et admettant un élément neutre  $e$ .

Les cinq propriétés suivantes sont vérifiées :

- 1) L'élément neutre  $e$  est le symétrique de lui même.
- 2) Si un élément  $x$  de  $E$  est symétrisable, et si  $x'$  est son symétrique alors  $x'$  est aussi symétrisable et son symétrique est égal à  $x$ .
- 3) Si  $x$  et  $y$  sont des éléments symétrisables de  $E$  alors  $x \star y$  est aussi symétrisable. Dans ce cas, si  $x'$  est le symétrique de  $x$  et si  $y'$  est le symétrique de  $y$  alors,  $y' \star x'$  est le symétrique de  $x \star y$ .
- 4) Soient  $x$  et  $y$  deux éléments de  $E$  qui commutent. Si  $x$  admet un symétrique  $x'$  alors  $x'$  commute avec  $y$ .
- 5) Soient  $x$  et  $y$  deux éléments de  $E$  qui commutent. Si  $x$  admet un symétrique  $x'$  et si  $y$  admet un symétrique  $y'$  alors  $x'$  et  $y'$  commutent.

### Démonstration :

- 1) Puisque  $e$  l'élément neutre de  $E$  alors  $e \star e = e$ .  
Donc  $e$  est le symétrique de lui même.
- 2) Soit  $x$  un élément symétrisable de  $E$ , et soit  $x'$  son symétrique.  
Puisque  $x' \star x = x \star x' = e$  alors  $x'$  est symétrisable, et son symétrique est égal à  $x$ .

3) Soient  $x$  et  $y$  deux éléments symétrisables de  $E$ ,  $x'$  le symétrique de  $x$  et  $y'$  le symétrique de  $y$ .

$$\begin{cases} (x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e \\ (y' * x') * (x * y) = y' * (x' * x) * y = y' * e * y = y' * y = e \end{cases}$$

Donc  $x * y$  est symétrisable et son symétrique est égal à  $y' * x'$ .

4) Supposons que  $x$  admet un symétrique  $x'$ .

$$\begin{aligned} x' * y &= (x' * y) * e = (x' * y) * (x * x') = x' * (y * x) * x' = x' * (x * y) * x' \\ &= (x' * x) * (y * x') = e * (y * x') \\ &= y * x' \end{aligned}$$

Alors  $x'$  commute avec  $y$ .

5) Supposons que  $x$  admet un symétrique  $x'$  et que  $y$  admet un symétrique  $y'$ .

D'après 4),  $x'$  commute avec  $y$ .

Puisque  $y$  et  $x'$  commutent, alors (d'après 4)),  $y'$  commute avec  $x'$ .

Donc  $x'$  et  $y'$  commutent.

### Remarque 1-3-4 :

Soit  $(E, .)$  un ensemble muni d'une loi de composition interne notée multiplicativement, associative et admettant un élément neutre  $e$ .

Les trois propriétés suivantes sont vérifiées :

- 1) Pour tout entier naturel  $n$ ,  $e^n = e$  (c'est à dire  $\forall n \in \mathbb{N} : e^n = e$ ).
- 2) Pour tout entier relatif  $n$ ,  $e^n = e$  (c'est à dire  $\forall n \in \mathbb{Z} : e^n = e$ ).
- 3) Si  $x$  est un élément inversible dans  $E$  alors son inverse est égal à  $x^{-1}$ .

### Démonstration :

1) Montrons par récurrence que pour tout entier naturel  $n$ ,  $e^n = e$ .

- **Pour  $n = 0$  :**

$$e^n = e^0 = e.$$

- **Pour  $n - 1$  :**

Supposons que  $e^{n-1} = e$ .

- **Pour  $n$  :**

Montrons qu'alors  $e^n = e$ .

$$\begin{aligned} e^n &= e^{n-1}e = ee \text{ (d'après l'hypothèse de récurrence)} \\ &= e. \end{aligned}$$

2) Soit  $n$  un entier relatif quelconque.

- **Si  $n \geq 0$  :**

Alors (d'après la propriété 1)) :  $e^n = e$ .

- **Pour  $n \leq 0$  :**

Alors :  $e^n = (e^{-1})^{-n} = e^{-n} = e$ .

3) Soit  $x$  un élément inversible de  $E$  et soit  $x'$  son inverse

$$x^{-1} = (x')^{-( -1)} = (x')^1 = x'. \text{ Donc } x^{-1} \text{ est l'inverse de } x.$$

### Remarque 1-3-5 :

Soit  $(E, +)$  un ensemble muni d'une loi de composition interne notée additivement, additivement, associative admettant un zéro.

Les trois propriétés suivantes sont vérifiées :

- 1) Pour tout entier naturel  $n$ ,  $n0_E = 0_E$  (c'est à dire  $\forall n \in \mathbb{N} : n0_E = 0_E$ ).
- 2) Pour tout entier relatif  $n$ ,  $n0_E = 0_E$  (c'est à dire  $\forall n \in \mathbb{Z} : n0_E = 0_E$ ).



- 3) Si  $x$  est un élément de  $E$  qui admet un opposé, son opposé est égal à  $(-1)x$ .  
C'est à dire, si  $x$  est un élément de  $E$  qui admet un opposé, alors :  $(-1)x = -x$ .

**Démonstration :**

- 1) Montrons par récurrence que pour tout entier naturel  $n$  :  $n0_E = 0_E$ .

- **Pour  $n = 0$  :**

$$n0_E = 00_E = 0_E.$$

- **Pour  $n - 1$  :**

Supposons que  $(n - 1)0_E = 0_E$ .

- **Pour  $n$  :**

Montrons qu'alors  $n0_E = 0_E$ .

$$\begin{aligned} n0_E &= (n - 1)0_E + 0_E = 0_E + 0_E \text{ (d'après l'hypothèse de récurrence)} \\ &= 0_E. \end{aligned}$$

- 2) Soit  $n$  un entier relatif quelconque.

- **Si  $n \geq 0$  :**

Alors (d'après la propriété i)) :  $n0_E = 0_E$ .

- **Pour  $n \leq 0$  :**

Alors :  $n0_E = (-n)(-0_E) = (-n)0_E = 0_E$ .

- 3) Soit  $x$  un élément de  $E$  qui admet un opposé.

$(-1)x = [ -(-1) ](-x) = 1(-x) = -x$ . Donc  $(-1)x$  est l'opposé de  $x$ .

**Proposition 1-3-6 :**

Soit  $E$  un ensemble muni d'une loi de composition interne associative et admettant un élément neutre.

Les propriétés suivantes sont vérifiées :

- 1) Si la loi de  $E$  est multiplicative et si  $x$  est un élément inversible de  $E$  alors,  
 $(x^{-1})^{-1} = x$ .
- 2) Si la loi de  $E$  est additive et si  $x$  est un élément de  $E$ , qui admet un opposé alors,  
 $-(-x) = x$ .
- 3) Si la loi de  $E$  est multiplicative, et si  $x, y$  sont des éléments inversibles de  $E$  alors,  $xy$  est inversible et on a :  $(xy)^{-1} = y^{-1}x^{-1}$ .
- 4) Si la loi de  $E$  est additive, et si  $x, y$  sont des éléments de  $E$  qui possèdent des opposés, alors  $x + y$  possède un opposé et on a :  $-(x + y) = -y - x$ .
- 5) Si la loi de  $E$  est multiplicative et si  $x$  est un élément de  $E$  alors :
  - a)  $\forall n, m \in \mathbb{N} : x^n x^m = x^{n+m}$ .
  - b)  $\forall n, m \in \mathbb{N} : (x^n)^m = x^{nm}$ .
- 6) Si la loi de  $E$  est additive et si  $x$  est un élément de  $E$  alors :
  - a)  $\forall n, m \in \mathbb{N} : nx + mx = (n + m)x$ .
  - b)  $\forall n, m \in \mathbb{N} : n(mx) = (nm)x$ .
- 7) Si la loi de  $E$  est multiplicative et si  $x, y$  sont des éléments de  $E$  qui commutent alors :
  - a) si  $x$  et  $y$  commutent alors, pour tout entier naturel  $n$ ,  $(xy)^n = x^n y^n$ .
  - b) pour tout entier naturel  $n$ ,  $x^n$  et  $y^m$  commutent.  
**En particulier :**  $\forall n, m \in \mathbb{N} : x^n$  et  $x^m$  commutent.
- 8) Si la loi de  $E$  est additive et si  $x, y$  sont des éléments de  $E$  qui commutent alors :
  - a) si  $x$  et  $y$  commutent alors :  $\forall n \in \mathbb{N} : n(x + y) = nx + ny$  et  $E$ .
  - b) pour tout entier naturel  $n$ ,  $nx$  et  $my$  commutent.  
**En particulier :**  $\forall n, m \in \mathbb{N} : nx$  et  $mx$  commutent.

### Démonstration :

- 1) Supposons que la loi de  $E$  est multiplicative et soit  $x$  est un élément inversible de  $E$ .  
Puisque  $x^{-1}$  est l'inverse de  $x$  (d'après la proposition 1-3-4-3)), alors (d'après la proposition 1-3-3-2)),  $x^{-1}$  est inversible et on a :  $(x^{-1})^{-1} = x$ .
- 2) Supposons que la loi de  $E$  est additive et soit  $x$  est un élément de  $E$  qui admet un opposé.  
Puisque  $-x$  est l'opposé de  $x$ , alors (d'après la proposition 1-3-3-2)),  $x + y$  admet un opposé et on a :  $-(-x) = x$ .
- 3) Supposons que la loi de  $E$  est multiplicative et soient  $x, y$  deux éléments inversibles de  $E$ .  
Puisque  $x^{-1}$  et  $y^{-1}$  sont les inverses, respectivement de  $x$  et  $y$  (d'après la proposition 1-3-4-3)), alors (d'après la proposition 1-3-3-3)),  $xy$  est inversible et on a :  
 $(xy)^{-1} = y^{-1}x^{-1}$ .
- 4) Supposons que la loi de  $E$  est additive et soient  $x, y$  deux éléments de  $E$  qui possèdent des opposés.  
Puisque  $-x$  et  $-y$  sont les opposés, respectivement de  $x$  et  $y$ , alors (d'après la proposition 1-3-3-3)),  $x + y$  admet un opposé et on a :  $-(x + y) = -y + (-x) = -y - x$ .
- 5) Supposons que la loi de  $E$  est multiplicative.  
Soient  $x$  est un élément de  $E$  et  $e$  l'élément neutre de  $E$ .

a)  $\forall n, m \in \mathbb{N}$  :

- **Si  $n = 0$  :**

$$x^n x^m = x^0 x^m = e x^m = x^m = x^{0+m} = x^{n+m}.$$

- **Si  $m = 0$  :**

$$x^n x^m = x^n x^0 = x^n e = x^n = x^{n+0} = x^{n+m}.$$

- **Si  $n \neq 0$  et si  $m \neq 0$  :**

$$\text{Alors (d'après la proposition 1-3-1-1)), } x^n x^m = x^{n+m}.$$

b)  $\forall n, m \in \mathbb{N}$  :

- **Si  $n = 0$  :**

$$(x^n)^m = (x^0)^m = e^m = e = e^0 = e^{0m} = x^{nm}.$$

- **Si  $m = 0$  :**

$$(x^n)^m = (x^n)^0 = e = e^0 = e^{n0} = x^{nm}.$$

- **Si  $n \neq 0$  et si  $m \neq 0$  :**

$$\text{Alors (d'après la proposition 1-3-1-2)), } (x^n)^m = x^{nm}.$$

- 6) Supposons que la loi de  $E$  est additive, et soit  $x$  est un élément de  $E$ .

a)  $\forall n, m \in \mathbb{N}$  :

- **Si  $n = 0$  :**

$$nx + mx = 0x + mx = 0_E + mx = mx = (0 + m)x = (n + m)x.$$

- **Si  $m = 0$  :**

$$nx + mx = nx + 0x = nx + 0_E = nx = (n + 0)x = (n + m)x.$$

- **Si  $n \neq 0$  et si  $m \neq 0$  :**

$$\text{Alors (d'après la proposition 1-3-2-1)), } nx + mx = (n + m)x.$$

b)  $\forall n, m \in \mathbb{N}$  :

- **Si  $n = 0$  :**

$$n(mx) = 0(mx) = 0_E = 0x = (0m)x = (nm)x.$$

- **Si  $m = 0$  :**

$$n(mx) = n(0x) = n0_E = 0_E = 0x = (n0)x = (nm)x.$$

- **Si  $n \neq 0$  et si  $m \neq 0$  :**

$$\text{Alors (d'après la proposition 1-3-2-2)), } n(mx) = (nm)x.$$

7) Supposons que la loi de  $E$  est multiplicative.

Soient  $x, y$  deux éléments de  $E$  qui commutent et  $e$  l'élément neutre de  $E$ .

a)  $\forall n \in \mathbb{N}$  :

- **Si  $n = 0$**  :

$$(xy)^n = (xy)^0 = e = ee = x^0 y^0 = x^n y^n.$$

- **Si  $n \neq 0$**  :

Alors (d'après la proposition 1-3-1-3)),  $(xy)^n = x^n y^n$ .

b)  $\forall n, m \in \mathbb{N}$  :

- **Si  $n = 0$**  :

Alors  $x^n = x^0 = e$  commute avec  $y^m$ .

- **Si  $m = 0$**  :

Alors  $x^n$  commute avec  $e = y^0 = e = y^m$ .

- **Si  $n \neq 0$  et  $m \neq 0$**  :

Alors (d'après la propriété 1-3-1-4))),  $x^n$  et  $y^m$  commutent.

**En particulier** :  $\forall n, m \in \mathbb{N}$  :  $x^n$  et  $x^m$  commutent (car  $x$  commute avec  $x$ ).

8) Supposons que la loi de  $E$  est additive.

Soient  $x, y$  deux éléments de  $E$  qui commutent.

a) - **Si  $n = 0$**  :

$$n(x + y) = 0(x + y) = 0_E = 0_E + 0_E = 0x + 0y = nx + ny.$$

- **Si  $n \neq 0$**  :

Alors (d'après la proposition 1-3-2-3)),  $n(x + y) = nx + ny$ .

b) - **Si  $n = 0$**  :

Alors  $nx = 00_E = 0_E$  commute avec  $my$ .

- **Si  $m = 0$**  :

Alors  $nx$  commute avec  $0_E = 0y = my$ .

- **Si  $n \neq 0$  et  $m \neq 0$**  :

Alors (d'après la propriété 1-3-2-4))),  $nx$  et  $my$  commutent.

**En particulier** :  $\forall n, m \in \mathbb{N}$  :  $nx$  et  $mx$  commutent (car  $x$  commute avec  $x$ ).

### Lemme 1-3-7 :

Soit  $(E, .)$  un ensemble muni d'une loi de composition interne notée multiplicativement, associative et admettant un élément neutre.

Les quatre propriétés suivantes sont vérifiées :

1) Si  $x$  est un élément inversible de  $E$  alors :  $\forall n, m \in \mathbb{Z}^-$  :  $x^n x^m = x^{n+m}$ .

2) Si  $x$  est un élément inversible de  $E$  alors pour tout entier naturel  $n$ ,  $x^n$  est inversible, et son inverse est égal à  $x^{-n}$ .

C'est à dire si  $x$  est un élément inversible de  $E$  alors,

$$\forall n \in \mathbb{N} : x^n \text{ est inversible} \quad \text{et} \quad (x^n)^{-1} = x^{-n}.$$

3) Si  $x$  est un élément inversible de  $E$  alors pour tout entier relatif  $n$ ,  $x^n$  est inversible, et son inverse est égal à  $x^{-n}$ .

C'est à dire si  $x$  est un élément inversible de  $E$  alors,

$$\forall n \in \mathbb{Z} : x^n \text{ est inversible} \quad \text{et} \quad (x^n)^{-1} = x^{-n}.$$

4) Si  $x$  et  $y$  sont des éléments inversibles de  $E$  qui commutent alors :

$$\forall n, m \in \mathbb{Z} : x^n \text{ et } y^m \text{ commutent.}$$

**En particulier** :  $\forall n, m \in \mathbb{Z} : x^n \text{ et } x^m \text{ commutent.}$

### Démonstration :

1) Soit  $x$  est un élément inversible de  $E$ .

$$\forall n, m \in \mathbb{Z}^- : x^n x^m = (x^{-1})^{-n} (x^{-1})^{-m} = (x^{-1})^{-n-m} = (x^{-1})^{-(n+m)} = x^{n+m}.$$

2) Soient  $x$  un élément inversible de  $E$  et  $n$  un entier naturel.

$$\text{Puisque } x \text{ et } x^{-1} \text{ commutent alors : } \begin{cases} x^n x^{-n} = x^n (x^{-1})^n = (x x^{-1})^n = e^n = e \\ x^{-n} x^n = (x^{-1})^n x^n = (x^{-1} x)^n = e^n = e \end{cases}.$$

Donc  $x^n$  est inversible et son inverse est égal à  $x^{-n}$ .

3) Soient  $x$  un élément inversible de  $E$  et  $n$  un entier relatif.

- Si  $n \geq 0$  :

Alors (d'après 2)),  $x^n$  est inversible et son inverse est égal à  $x^{-n}$ .

- Si  $n \leq 0$  :

Alors  $-n \geq 0$  et par suite (d'après 2)),  $x^{-n}$  est inversible et son inverse est égal à  $x^{-(-n)} = x^n$ .

Puisque  $x^n$  est l'inverse de  $x^{-n}$  alors  $x^n$  est inversible et son inverse est égal à  $x^{-n}$ .

4) Soient  $x$  et  $y$  deux éléments inversibles de  $E$  qui commutent.

$\forall n, m \in \mathbb{Z}$  :

- Si  $n \geq 0$  et  $m \geq 0$  :

Alors (d'après la proposition 1-3-6-7) b)),  $x^n$  et  $y^m$  commutent.

- Si  $n \leq 0$  et  $m \leq 0$  :

Alors  $-n$  et  $-m$  sont positifs.

D'après la proposition 1-3-3-5)),  $x^{-1}$  et  $y^{-1}$  commutent (car  $x$  et  $y$  commutent).

Ce qui montre (d'après la proposition 1-3-6-7) b)), que,

$$x^n = (x^{-1})^{-n} \text{ et } y^m = (y^{-1})^{-m} \text{ commutent.}$$

- Si  $n \geq 0$  et  $m \leq 0$  :

Alors  $n$  et  $-m$  sont positifs.

D'après la proposition 1-3-3-4)),  $y^{-1}$  et  $x$  commutent (car  $y$  et  $x$  commutent).

Ce qui montre (d'après la proposition 1-3-6-7) b)), que  $x^n$  et  $y^m = (y^{-1})^{-m}$  commutent.

- Si  $n \leq 0$  et  $m \geq 0$  :

Alors  $-n$  et  $m$  sont positifs.

D'après la proposition 1-3-3-4)),  $x^{-1}$  et  $y$  commutent (car  $x$  et  $y$  commutent).

Ce qui montre (d'après la proposition 1-3-6-7) b)), que  $x^n = (x^{-1})^{-n}$  et  $y^m$  commutent.

### En particulier :

$\forall n, m \in \mathbb{Z} : x^n$  et  $x^m$  commutent (car  $x$  commute avec  $x$  lui même).

### Théorème 1-3-8 :

Soit  $(E, .)$  un ensemble muni d'une loi de composition interne notée multiplicativement, associative et admettant un élément neutre.

Les propriétés suivantes sont vérifiées :

1) Si  $x$  est un élément inversible de  $E$ , alors :

a)  $\forall n, m \in \mathbb{Z} : x^n x^m = x^{n+m}.$

b)  $\forall n, m \in \mathbb{Z} : (x^n)^m = x^{nm}.$

2) Si  $x$  et  $y$  sont des éléments inversibles de  $E$  qui commutent alors :

$$\forall n \in \mathbb{Z} : (xy)^n = x^n y^n.$$

### Démonstration :

1) Soient  $x$  un élément inversible de  $E$  et  $e$  l'élément neutre de  $E$ .

a)  $\forall n, m \in \mathbb{Z}$  :

- **Si  $n \geq 0$  et  $m \geq 0$  :**

Alors (d'après la proposition 1-3-6-5) a)), on a :  $x^n x^m = x^{n+m}$ .

- **Si  $n \leq 0$  et  $m \leq 0$  :**

Alors  $-n \geq 0$  et  $-m \geq 0$ .

Par suite on a :

$$\begin{aligned} x^n x^m &= (x^{-1})^{-n} (x^{-1})^{-m} \\ &= (x^{-1})^{-n-m} \quad (\text{d'après la proposition 1-3-6-5) a)) \\ &= (x^{-1})^{-(n+m)} \\ &= x^{n+m}. \end{aligned}$$

- **Si  $n \geq 0, m \leq 0$  et  $n + m \geq 0$  :**

Alors  $n \geq 0, -m \geq 0$  et  $n + m \geq 0$ . Par suite on a :

$$\begin{aligned} x^n x^m &= x^{n+m-m} x^m = (x^{n+m} x^{-m}) x^m \quad (\text{d'après la proposition 1-3-6-5) a)) \\ &= x^{n+m} (x^{-m} x^m) \\ &= x^{n+m} e \quad (\text{d'après le lemme 1-3-7-3)) \\ &= x^{n+m}. \end{aligned}$$

- **Si  $n \geq 0, m \leq 0$  et  $n + m \leq 0$  :**

Alors  $-n \leq 0, m \leq 0$  et  $n + m \leq 0$ . Par suite on a :

$$\begin{aligned} x^n x^m &= x^n x^{-n+n+m} = x^n (x^{-n} x^{n+m}) \quad (\text{d'après le lemme 1-3-7-1)) \\ &= (x^n x^{-n}) x^{n+m} \\ &= e x^{n+m} \quad (\text{d'après le lemme 1-3-7-3)) \\ &= x^{n+m}. \end{aligned}$$

- **Si  $n \leq 0, m \geq 0$  et  $n + m \geq 0$  :**

Alors  $-n \geq 0, m \geq 0$  et  $n + m \geq 0$ . Par suite on a :

$$\begin{aligned} x^n x^m &= x^n x^{-n+n+m} = x^n (x^{-n} x^{n+m}) \quad (\text{d'après la proposition 1-3-6-5) a)) \\ &= (x^n x^{-n}) x^{n+m} \\ &= e x^{n+m} \quad (\text{d'après le lemme 1-3-7-3)) \\ &= x^{n+m}. \end{aligned}$$

- **Si  $n \leq 0, m \geq 0$  et  $n + m \leq 0$  :**

Alors  $n \leq 0, -m \leq 0$  et  $n + m \leq 0$ . Par suite on a :

$$\begin{aligned} x^n x^m &= x^{n+m-m} x^m \\ &= (x^{n+m} x^{-m}) x^m \quad (\text{d'après le lemme 1-3-7-1)) \\ &= x^{n+m} (x^{-m} x^m) \\ &= x^{n+m} e \quad (\text{d'après le lemme 1-3-7-3)) \\ &= x^{n+m}. \end{aligned}$$

On a donc montrer que :  $\forall n, m \in \mathbb{Z} : x^n x^m = x^{n+m}$ .

b)  $\forall n, m \in \mathbb{Z}$  :

- **Si  $n \geq 0$  et  $m \geq 0$  :**

Alors (d'après la proposition 1-3-6-5) b)), on a :  $(x^n)^m = x^{nm}$ .

- **Si  $n \geq 0$  et  $m \leq 0$  :**

Alors (d'après la proposition 1-3-7-3) ), on a :  $(x^n)^m = [(x^n)^{-m}]^{-1}$ .

D'après la proposition 1-3-6-5) b)), on donc :

$$(x^n)^m = (x^{n(-m)})^{-1} = (x^{-nm})^{-1} = x^{nm} \quad (\text{d'après la proposition 1-3-7-3}).$$

- **Si  $n \leq 0$  et  $m \geq 0$  :**

$$\begin{aligned}(x^n)^m &= [(x^{-1})^{-n}]^m = (x^{-1})^{(-n)m} \quad (\text{d'après la proposition 1-3-6-5 b)}) \\ &= (x^{-1})^{-nm} = x^{-(-nm)} \\ &= x^{nm}.\end{aligned}$$

- **Si  $n \leq 0$  et  $m \leq 0$  :**

Alors  $n \leq 0$  et  $-m \geq 0$  Par suite on a :

$$\begin{aligned}(x^n)^m &= [(x^n)^{-m}]^{-1} \quad (\text{d'après la proposition 1-3-7-3}) \\ &= [[(x^{-1})^{-n}]^{-m}]^{-1} \\ &= [(x^{-1})^{(-n)(-m)}]^{-1} \quad (\text{d'après la proposition 1-3-6-5 b)}) \\ &= [(x^{-1})^{nm}]^{-1} \\ &= (x^{-1})^{-nm} \quad (\text{d'après la proposition 1-3-7-3}) \\ &= x^{-(-nm)} \\ &= x^{nm}.\end{aligned}$$

On a donc montré que :  $\forall n, m \in \mathbb{Z} : x^n x^m = x^{n+m}$ .

2) Soient  $x$  et  $y$  deux éléments inversibles de  $E$  qui commutent.

$\forall n \in \mathbb{Z} :$

- **Si  $n \geq 0$  :**

Alors (d'après la proposition 1-3-6-7 a)), on a :  $(xy)^n = x^n y^n$ .

- **Si  $n \leq 0$  :**

Puisque  $x$  et  $y$  commutent alors (d'après la proposition 1-3-3-5)),  $x^{-1}$  et  $y^{-1}$  commutent.

Par suite on a :

$$\begin{aligned}(xy)^n &= [(xy)^{-1}]^{-n} = [(yx)^{-1}]^{-n} \\ &= (x^{-1}y^{-1})^{-n} \quad (\text{d'après la proposition 1-3-3-3)}) \\ &= (x^{-1})^{-n}(y^{-1})^{-n} \quad (\text{d'après la proposition 1-3-6-7 a)}), \\ &= x^n y^n.\end{aligned}$$

### **Lemme 1-3-9 :**

Soit  $(E, +)$  un ensemble muni d'une loi de composition interne notée additivement, associative et admettant un zéro.

Les quatre propriétés suivantes sont vérifiées :

1) Si  $x$  est un élément de  $E$  qui admet un opposé alors :

$$\forall n, m \in \mathbb{Z}^- : nx + mx = (n + m)x.$$

2) Si  $x$  est un élément de  $E$  qui admet un opposé alors pour tout entier naturel  $n$ ,  $nx$  admet un opposé, et son opposé est égal à  $(-n)x$ .

C'est à dire si  $x$  est un élément de  $E$  qui admet un opposé alors,

$$\forall n \in \mathbb{N} : nx \text{ admet un opposé} \quad \text{et} \quad -nx = (-n)x.$$

3) Si  $x$  est un élément de  $E$  qui admet un opposé alors pour tout entier relatif  $n$ ,  $nx$  admet un opposé, et son opposé est égal à  $(-n)x$ .

C'est à dire si  $x$  est un élément de  $E$  qui admet un opposé alors,

$$\forall n \in \mathbb{Z} : nx \text{ admet un opposé} \quad \text{et} \quad -nx = (-n)x.$$

4) Si  $x$  et  $y$  sont des éléments de  $E$  qui commutent qui possèdent des opposés alors :

$$\forall n, m \in \mathbb{Z} : nx \text{ et } my \text{ commutent.}$$

**En particulier :**  $\forall n, m \in \mathbb{Z} : nx$  et  $mx$  commutent.

**Démonstration :**

1) Soit  $x$  un élément de  $E$  qui admet un opposé.

$$\forall n, m \in \mathbb{Z}^- : nx + mx = (-n)(-x) + (-m)(-x) = (-n - m)(-x) = [-(n + m)](-x) = (n + m)x.$$

2) Soient  $x$  un élément de  $E$  qui admet un opposé et  $n$  un entier naturel.

Puisque  $x$  et  $-x$  commutent alors :

$$\begin{cases} nx + (-n)x = nx + n(-x) = n(x - x) = n0_E = 0_E \\ (-n)x + nx = n(-x) + nx = n(-x + x) = n0_E = 0_E \end{cases}.$$

Donc  $nx$  admet un opposé qui est égal à  $(-n)x$ .

3) Soient  $x$  un élément de  $E$  qui admet un opposé et  $n$  un entier relatif.

- **Si  $n \geq 0$  :**

Alors (d'après 2)),  $nx$  admet un opposé qui est égal à  $(-n)x$ .

- **Si  $n \leq 0$  :**

Alors  $-n \geq 0$  et par suite (d'après 2)),  $(-n)x$  admet un opposé qui est égal à  $[-(-n)]x = nx$ .

Puisque  $nx$  est l'opposé de  $(-n)x$  alors  $nx$  admet un opposé qui est égal à  $(-n)x$ .

4) Soient  $x$  et  $y$  deux éléments de  $E$  qui possèdent des opposés et qui commutent.

$\forall n, m \in \mathbb{Z} :$

- **Si  $n \geq 0$  et  $m \geq 0$  :**

Alors (d'après la proposition 1-3-6-8) b)),  $nx$  et  $my$  commutent.

- **Si  $n \leq 0$  et  $m \leq 0$  :**

Alors  $-n$  et  $-m$  sont positifs.

D'après la proposition 1-3-3-5)),  $-x$  et  $-y$  commutent (car  $x$  et  $y$  commutent).

Ce qui montre (d'après la proposition 1-3-6-8) b)), que,

$$nx = (-n)(-x) \text{ et } my = (-m)(-y) \text{ commutent.}$$

- **Si  $n \geq 0$  et  $m \leq 0$  :**

Alors  $n$  et  $-m$  sont positifs.

D'après la proposition 1-3-3-4)),  $-y$  et  $x$  commutent (car  $y$  et  $x$  commutent).

Ce qui montre (d'après la proposition 1-3-6-8) b)), que  $nx$  et  $my = (-m)(-y)$  commutent.

- **Si  $n \leq 0$  et  $m \geq 0$  :**

Alors  $-n$  et  $m$  sont positifs.

D'après la proposition 1-3-3-4)),  $-x$  et  $y$  commutent (car  $x$  et  $y$  commutent).

Ce qui montre (d'après la proposition 1-3-6-8) b)), que  $nx = (-n)(-x)$  et  $my$  commutent.

**En particulier :**

$\forall n, m \in \mathbb{Z} : nx$  et  $mx$  commutent (car  $x$  commute avec  $x$  lui même).

**Théorème 1-3-10 :**

Soit  $(E, +)$  un ensemble muni d'une loi de composition interne notée additivement, associative et admettant un zéro.

Les propriétés suivantes sont vérifiées :

1) Si  $x$  est un élément de  $E$  qui admet un opposé alors :

a)  $\forall n, m \in \mathbb{Z} : nx + mx = (n + m)x.$

b)  $\forall n, m \in \mathbb{Z} : n(mx) = (nm)x.$

2) Si  $x$  et  $y$  sont des éléments de  $E$  qui possèdent des opposés et qui commutent alors :  $\forall n \in \mathbb{Z} : n(x + y) = nx + ny.$

### Démonstration :

1) Soient  $x$  un élément de  $E$  qui admet un opposé.

a)  $\forall n, m \in \mathbb{Z}$  :

- **Si  $n \geq 0$  et  $m \geq 0$  :**

Alors (d'après la proposition 1-3-6-6) a)), on a :  $nx + mx = (n + m)x$ .

- **Si  $n \leq 0$  et  $m \leq 0$  :**

Alors  $-n \geq 0$  et  $-m \geq 0$ .

Par suite on a :

$$\begin{aligned} nx + mx &= (-n)(-x) + (-m)(-x) \\ &= (-n - m)(-x) \quad (\text{d'après la proposition 1-3-6-6) a))} \\ &= [-(n + m)](-x) \\ &= (n + m)x. \end{aligned}$$

- **Si  $n \geq 0$ ,  $m \leq 0$  et  $n + m \geq 0$  :**

Alors  $n \geq 0$ ,  $-m \geq 0$  et  $n + m \geq 0$ . Par suite on a :

$$\begin{aligned} nx + mx &= (n + m - m)x + mx \\ &= [(n + m)x + (-m)x] + mx \quad (\text{d'après la proposition 1-3-6-6) a))} \\ &= (n + m)x + [(-m)x + mx] \\ &= (n + m)x + 0_E \quad (\text{d'après le lemme 1-3-9-3))} \\ &= (n + m)x. \end{aligned}$$

- **Si  $n \geq 0$ ,  $m \leq 0$  et  $n + m \leq 0$  :**

Alors  $-n \leq 0$ ,  $m \leq 0$  et  $n + m \leq 0$ . Par suite on a :

$$\begin{aligned} nx + mx &= nx + (-n + n + m)x \\ &= nx + [(-n)x + (n + m)x] \quad (\text{d'après le lemme 1-3-9-1))} \\ &= [nx + (-n)x] + (n + m)x \\ &= 0_E + (n + m)x \quad (\text{d'après le lemme 1-3-9-3))} \\ &= (n + m)x. \end{aligned}$$

- **Si  $n \leq 0$ ,  $m \geq 0$  et  $n + m \geq 0$  :**

Alors  $-n \geq 0$ ,  $m \geq 0$  et  $n + m \geq 0$ . Par suite on a :

$$\begin{aligned} nx + mx &= nx + (-n + n + m)x \\ &= nx + [(-n)x + (n + m)x] \quad (\text{d'après la proposition 1-3-6-6) a))} \\ &= [nx + (-n)x] + (n + m)x \\ &= 0_E + (n + m)x \quad (\text{d'après le lemme 1-3-9-3))} \\ &= (n + m)x. \end{aligned}$$

- **Si  $n \leq 0$ ,  $m \geq 0$  et  $n + m \leq 0$  :**

Alors  $n \leq 0$ ,  $-m \leq 0$  et  $n + m \leq 0$ . Par suite on a :

$$\begin{aligned} nx + mx &= (n + m - m)x + mx \\ &= [(n + m)x + (-m)x] + mx \quad (\text{d'après le lemme 1-3-9-1))} \\ &= (n + m)x + [(-m)x + mx] \\ &= (n + m)x + 0_E \quad (\text{d'après le lemme 1-3-9-3))} \\ &= (n + m)x. \end{aligned}$$

On a donc montré que :  $\forall n, m \in \mathbb{Z} : nx + mx = (n + m)x$ .

b)  $\forall n, m \in \mathbb{Z}$  :

- **Si  $n \geq 0$  et  $m \geq 0$  :**

Alors (d'après la proposition 1-3-6-6) b)), on a :  $n(mx) = (nm)x$ .



- **Si  $n \geq 0$  et  $m \leq 0$  :**

Alors  $n \geq 0$  et  $-m \geq 0$ . Par suite on a :

$$\begin{aligned} n(mx) &= n[(-m)(-x)] \\ &= [n(-m)](-x) \quad (\text{d'après la proposition 1-3-6-6 b)}) \\ &= (-nm)(-x) = [-(nm)]x \\ &= (nm)x. \end{aligned}$$

- **Si  $n \leq 0$  et  $m \geq 0$  :**

Alors  $-n \geq 0$  et  $m \geq 0$ . Par suite on a :

$$\begin{aligned} n(mx) &= -[-n(mx)] \\ &= -[(-n)(mx)] \quad (\text{d'après la proposition 1-3-9-3))} \\ &= -[(-nm)x] \quad (\text{d'après la proposition 1-3-6-6 b)}) \\ &= [-(nm)]x \quad (\text{d'après la proposition 1-3-9-3))} \\ &= (nm)x. \end{aligned}$$

- **Si  $n \leq 0$  et  $m \leq 0$  :**

Alors  $-n \geq 0$  et  $-m \geq 0$ . Par suite on a :

$$\begin{aligned} n(mx) &= -[-n(mx)] \\ &= -[(-n)(mx)] \quad (\text{d'après la proposition 1-3-9-3))} \\ &= -[(-n)[(-m)(-x)]] \\ &= -[(-n)(-m)(-x)] \quad (\text{d'après la proposition 1-3-6-6 b)}) \\ &= -[(nm)(-x)] = -[(-nm)x] \\ &= [-(nm)]x \quad (\text{d'après la proposition 1-3-9-3))} \\ &= (nm)x. \end{aligned}$$

On a donc montré que :  $\forall n, m \in \mathbb{Z} : n(mx) = (nm)x$ .

2) Soient  $x$  et  $y$  deux éléments de  $E$  qui possèdent des opposés et qui commutent.

$\forall n \in \mathbb{Z} :$

- **Si  $n \geq 0$  :**

Alors (d'après la proposition 1-3-6-8 a)), on a :  $n(x + y) = nx + ny$ .

- **Si  $n \leq 0$  :**

Puisque  $x$  et  $y$  commutent alors (d'après la proposition 1-3-3-5)),  $-x$  et  $-y$  commutent.

Par suite on a :

$$\begin{aligned} n(x + y) &= (-n)[-(x + y)] = (-n)[-(y + x)] \\ &= (-n)(-x - y) \quad (\text{d'après la proposition 1-3-3-3))} \\ &= (-n)[-x + (-y)] \\ &= (-n)(-x) + (-n)(-y) \quad (\text{d'après la proposition 1-3-6-8 a)}) \\ &= nx + ny. \end{aligned}$$

### Proposition 1-3-11 :

Soient  $(E, *)$ ,  $(F, T)$  et  $(G, \perp)$  des ensembles munis des lois de composition internes respectivement  $*$ ,  $T$  et  $\perp$ .

Si  $f$  est un homomorphisme de  $(E, *)$  vers  $(F, T)$  et si  $g$  est un homomorphisme de  $(F, T)$  vers  $(G, \perp)$  alors,  $g \circ f$  est un homomorphisme de  $(E, *)$  vers  $(G, \perp)$ .

**Démonstration :**

Soient  $f$  un homomorphisme de  $(E, *)$  vers  $(F, T)$  et  $g$  un homomorphisme de  $(F, T)$  vers  $(G, \perp)$ .

$$\begin{aligned}\forall x, y \in E : (g \circ f)(x \star y) &= g(f(x \star y)) = g(f(x)Tf(y)) = g(f(x)) \perp g(f(y)) \\ &= (g \circ f)(x) \perp (g \circ f)(y).\end{aligned}$$

Donc  $g \circ f$  est un homomorphisme de  $(E, *)$  vers  $(G, \perp)$ .

**Proposition 1-3-12 :**

Soient  $(E, *)$  et  $(F, T)$  deux ensembles munis des lois de composition internes respectivement  $*$  et  $T$ .

Si  $f$  est un isomorphisme de  $(E, *)$  vers  $(F, T)$  alors,  $f^{-1}$  est un isomorphisme de  $(F, T)$  vers  $(E, *)$ .

**Démonstration :**

Soit  $f$  un isomorphisme de  $(E, *)$  vers  $(F, T)$ .

Soient  $x$  et  $y$  deux éléments quelconques de  $F$ .

Posons  $f^{-1}(x) = a$  et  $f^{-1}(y) = b$ . Alors,  $x = f(a)$  et  $y = f(b)$ .

$$\begin{aligned}f^{-1}(xTy) &= f^{-1}(f(a)Tf(b)) = f^{-1}(f(a \star b)) = (f^{-1} \circ f)(a \star b) = id_E(a \star b) = a \star b \\ &= f^{-1}(x) \star f^{-1}(y).\end{aligned}$$

Donc  $f^{-1}$  est un homomorphisme bijective de  $(F, T)$  vers  $(E, *)$ .

Ce qui montre que  $f^{-1}$  est un isomorphisme de  $(F, T)$  vers  $(E, *)$ .

**Proposition 1-3-13 :**

Soient  $(E, *)$  et  $(F, T)$  deux ensembles munis des lois de composition internes respectivement  $*$  et  $T$ .

Si  $f$  est un homomorphisme de  $(E, *)$  vers  $(F, T)$ , alors les six propriétés suivantes sont vérifiées :

$$1) \forall x_1, x_2, \dots, x_n \in E : f\left(\star_{i=1}^n x_i\right) = T_{i=1}^n f(x_i).$$

**En particulier :**

a) Si les deux lois de composition internes de  $E$  et  $F$  sont multiplicatives alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\prod_{i=1}^n x_i\right) = \prod_{i=1}^n f(x_i).$$

b) Si les deux lois de composition internes de  $E$  et  $F$  sont additives alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\sum_{i=1}^n x_i\right) = \sum_{i=1}^n f(x_i).$$

c) Si la loi de composition interne de  $E$  est multiplicative et si la loi de composition interne de  $F$  est additive alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\prod_{i=1}^n x_i\right) = \sum_{i=1}^n f(x_i).$$

d) Si la loi de composition interne de  $E$  est additive et si la loi de composition interne de  $F$  est multiplicative alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\sum_{i=1}^n x_i\right) = \prod_{i=1}^n f(x_i).$$

2) Si les deux lois de composition internes de  $E$  et  $F$  sont multiplicatives alors :

$$\forall x \in E \quad \text{et} \quad \forall n \in \mathbb{N}^* : f(x^n) = f(x)^n.$$

- 3) Si les deux lois de composition internes de  $E$  et  $F$  sont additives alors :
- $$\forall x \in E \text{ et } \forall n \in \mathbb{N}^* : f(nx) = nf(x).$$
- 4) Si la loi de composition interne de  $E$  est multiplicative et si la loi de composition interne de  $F$  est additive alors :
- $$\forall x \in E \text{ et } \forall n \in \mathbb{N}^* : f(x^n) = nf(x)$$
- 5) Si la loi de composition interne de  $E$  est additive et si la loi de composition interne de  $F$  est multiplicative alors :
- $$\forall x \in E \text{ et } \forall n \in \mathbb{N}^* : f(nx) = f(x)^n$$
- 6) Si  $E$  admet un élément neutre  $e$  et si  $F$  admet un élément neutre  $\varepsilon$  alors on a pas on a pas forcément  $f(e) = \varepsilon$ .

### Démonstration :

Soit  $f$  un homomorphisme de  $(E, *)$  vers  $(F, T)$ .

- 1) Montrons par récurrence que pour tout entier naturel non nul  $n$ , si  $x_1, \dots, x_n$  sont des éléments quelconques de  $E$  alors :  $f(\star_{i=1}^n x_i) = T_{i=1}^n f(x_i)$ .

- **Pour  $n = 1$  :**

$$\forall x_1, \dots, x_n \in E : f(\star_{i=1}^n x_i) = f(\star_{i=1}^1 x_i) = f(x_1) = T_{i=1}^1 f(x_i) = T_{i=1}^n f(x_i).$$

- **Pour  $n - 1$  :**

Supposons que si  $x_1, \dots, x_{n-1}$  sont des éléments quelconques de  $E$  alors :

$$f(\star_{i=1}^{n-1} x_i) = T_{i=1}^{n-1} f(x_i).$$

- **Pour  $n$  :**

Montrons qu'alors si  $x_1, \dots, x_n$  sont des éléments quelconques de  $E$  alors :

$$f(\star_{i=1}^n x_i) = T_{i=1}^n f(x_i).$$

Soient  $x_1, \dots, x_n$  des éléments quelconques de  $E$ .

$$f(\star_{i=1}^n x_i) = f((\star_{i=1}^{n-1} x_i) \star x_n) = f(\star_{i=1}^{n-1} x_i) T f(x_n) = [T_{i=1}^{n-1} f(x_i)] T f(x_n) = T_{i=1}^n f(x_i).$$

### En particulier :

- a) Si les deux lois de composition internes de  $E$  et  $F$  sont multiplicatives alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\prod_{i=1}^n x_i\right) = \prod_{i=1}^n f(x_i).$$

- b) Si les deux lois de composition internes de  $E$  et  $F$  sont additives alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\sum_{i=1}^n x_i\right) = \sum_{i=1}^n f(x_i).$$

- c) Si la loi de composition interne de  $E$  est multiplicative et si la loi de composition interne de  $F$  est additive alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\prod_{i=1}^n x_i\right) = \sum_{i=1}^n f(x_i).$$

- d) Si la loi de composition interne de  $E$  est additive et si la loi de composition interne de  $F$  est multiplicative alors :

$$\forall x_1, x_2, \dots, x_n \in E : f\left(\sum_{i=1}^n x_i\right) = \prod_{i=1}^n f(x_i).$$

- 2) Supposons que les deux lois de composition internes de  $E$  et  $E'$  sont multiplicatives. Soit  $x$  un élément quelconque de  $E$  et  $n$  un entier naturel non nul quelconque.

Pour tout entier naturel  $i = 1, \dots, n$  posons  $x_i = x$ .

$$f(x^n) = f\left(\prod_{i=1}^n x_i\right) = \prod_{i=1}^n f(x_i) = f(x)^n.$$

- 3) Supposons que les deux lois de composition internes de  $E$  et  $E'$  sont additives.  
 Soit  $x$  un élément quelconque de  $E$  et  $n$  un entier naturel non nul quelconque.  
 Pour tout entier naturel  $i = 1, \dots, n$  posons  $x_i = x$ .

$$f(nx) = f\left(\sum_{i=1}^n x_i\right) = \sum_{i=1}^n f(x_i) = nf(x).$$

- 4) Supposons que la loi de composition interne de  $E$  est multiplicative et que la loi de composition interne de  $E'$  est additive.

Soit  $x$  un élément quelconque de  $E$  et  $n$  un entier naturel non nul quelconque.

Pour tout entier naturel  $i = 1, \dots, n$  posons  $x_i = x$ .

$$f(x^n) = f\left(\prod_{i=1}^n x_i\right) = \sum_{i=1}^n f(x_i) = nf(x).$$

- 5) Supposons que la loi de composition interne de  $E$  est additive et que la loi de composition interne de  $E'$  est multiplicative.

Soit  $x$  un élément quelconque de  $E$  et  $n$  un entier naturel non nul quelconque.

Pour tout entier naturel  $i = 1, \dots, n$  posons  $x_i = x$ .

$$f(nx) = f\left(\sum_{i=1}^n x_i\right) = \prod_{i=1}^n f(x_i) = f(x)^n.$$

#### 6) Contre exemple :

Supposons que  $E = F = \mathbb{R} \times \mathbb{R}$ . On munit  $E = F = \mathbb{R} \times \mathbb{R}$  de la multiplication.

$(1, 1)$  est l'élément neutre de  $E$  et  $F$ .

Soit  $f$  l'application de  $E$  vers  $E'$  définie par :  $f : E = \mathbb{R} \times \mathbb{R} \rightarrow F = \mathbb{R} \times \mathbb{R}$

$$a = (x, y) \mapsto f(a) = (x, 0)$$

$\forall a = (x, y) \in E = \mathbb{R} \times \mathbb{R}$  et  $\forall b = (z, t) \in E = \mathbb{R} \times \mathbb{R}$  :

$$f(ab) = f((x, y)(z, t)) = f((xz, yt)) = (xz, 0) = (xz, 00) = (x, 0)(z, 0) = f(a)f(b).$$

Donc  $f$  est un homomorphisme de  $(E, \cdot)$  vers  $(F, \cdot)$  mais  $f((1, 1)) = (1, 0) \neq (1, 1)$ .

C'est à dire que  $f$  est un homomorphisme de  $(E, \cdot)$  vers  $(F, \cdot)$  mais l'image de l'élément neutre de  $E$  par  $f$  n'est pas égal à l'élément neutre de  $F$ .

Ce qui montre que si  $E$  admet un élément neutre  $e$  et si  $F$  admet un élément neutre  $\varepsilon$  alors on a pas forcément  $f(e) = \varepsilon$ .

#### Lemme 1-3-14 :

Soit  $(E, \star)$  un ensemble muni d'une loi de composition interne  $\star$  associative.

Si  $a, b_1, \dots, b_n$  sont des éléments quelconques de  $E$  et si l'élément  $a$  commute avec chacun des éléments  $b_1, \dots, b_n$ , alors  $a$  commute avec l'élément  $\star_{i=1}^n b_i$ .

#### Démonstration :

Montrons par récurrence que pour tout entier naturel non nul  $n$ , si  $a, b_1, \dots, b_n$  sont des éléments quelconques de  $E$  et si l'élément  $a$  commute avec chacun des éléments  $b_1, \dots, b_n$ , alors  $a$  commute avec l'élément  $\star_{i=1}^n b_i$ .

– **Pour  $n = 1$  :**

Soient  $a, b_1, \dots, b_n$  des éléments quelconques de  $E$  tels que  $a$  commute avec chacun des éléments  $b_1, \dots, b_n$ .

$a$  commute avec  $b_1 = \star_{i=1}^1 b_i = \star_{i=1}^n b_i$ .

– **Pour  $n - 1$  :**

Supposons que si  $a, b_1, \dots, b_{n-1}$  sont des éléments quelconques de  $E$  et si  $a$  commute avec chacun des éléments  $b_1, \dots, b_{n-1}$  alors  $a$  commute avec l'élément  $\star_{i=1}^{n-1} b_i$ .

– **Pour  $n$  :**

Montrons qu'alors si  $a, b_1, \dots, b_n$  sont des éléments quelconques de  $E$  et si l'élément  $a$  commute avec chacun des éléments  $b_1, \dots, b_n$ , alors  $a$  commute avec l'élément

$$\begin{aligned} & \star_{i=1}^n b_i. \\ a \star (\star_{i=1}^n b_i) &= a \star [(\star_{i=1}^{n-1} b_i) \star b_n] = [a \star (\star_{i=1}^{n-1} b_i)] \star b_n \\ &= [(\star_{i=1}^{n-1} b_i) \star a] \star b_n \quad (\text{d'après l'hypothèse de récurrence}) \\ &= (\star_{i=1}^{n-1} b_i) \star (a \star b_n) = (\star_{i=1}^{n-1} b_i) \star (b_n \star a) = [(\star_{i=1}^{n-1} b_i) \star b_n] \star a \\ &= (\star_{i=1}^n b_i) \star a. \end{aligned}$$

Donc  $a$  commute avec l'élément  $\star_{i=1}^n b_i$ .

**Lemme 1-3-15 :**

Soient  $(E, \star)$  un ensemble muni d'une loi de composition interne  $\star$  associative, et  $a_1, \dots, a_n, b_1, \dots, b_m$  des éléments quelconques de  $E$

Si chacun des éléments  $a_1, \dots, a_n$  commute avec chacun des éléments  $b_1, \dots, b_m$ , alors l'élément  $\star_{i=1}^n a_i$  commute avec l'élément  $\star_{i=1}^m b_i$ .

**Démonstration :**

Supposons que chacun des éléments  $a_1, \dots, a_n$  commute avec chacun des éléments  $b_1, \dots, b_m$ .

Donc (d'après le lemme précédent 1-3-14), chacun des éléments  $b_1, \dots, b_m$  commute avec chacun l'élément  $\star_{i=1}^n a_i$ .

Puisque l'élément  $\star_{i=1}^n a_i$  commute avec chacun des éléments  $b_1, \dots, b_m$  alors (d'après le lemme 1-3-14), l'élément  $\star_{i=1}^n a_i$  commute avec l'élément  $\star_{i=1}^m b_i$ .

**Lemme 1-3-16 :**

Soient  $(E, \star)$  un ensemble muni d'une loi de composition interne  $\star$  associative, et  $a_1, a_2, \dots, a_n$  des éléments quelconques de  $E$  (où  $n \geq 2$ ) qui commutent deux à deux.

Pour tout entier naturel  $k = 1, \dots, n-1$ , si  $b_1, b_2, \dots, b_n$  sont les éléments de  $E$

$$\text{tels que : } \forall i = 1, 2, \dots, n : \begin{cases} b_i = a_i & \text{si } i \neq n \text{ et } i \neq k \\ b_n = a_k & \text{si } i = n \\ b_k = a_n & \text{si } i = k \end{cases}, \text{ alors :}$$

$b_1, b_2, \dots, b_n$  commutent deux à deux et on a :  $\star_{i=1}^n a_i = \star_{i=1}^n b_i$ .

**Démonstration :**

Soit  $k$  un élément quelconque de l'ensemble  $\{1, \dots, n-1\}$  et soient  $b_1, b_2, \dots, b_n$  les

$$\text{éléments de } E \text{ tels que : } \forall i = 1, 2, \dots, n : \begin{cases} b_i = a_i & \text{si } i \neq n \text{ et } i \neq k \\ b_n = a_k & \text{si } i = n \\ b_k = a_n & \text{si } i = k \end{cases}.$$

Puisque  $b_1, b_2, \dots, b_n$  sont les éléments  $a_1, a_2, \dots, a_n$  et puisque  $a_1, a_2, \dots, a_n$  commutent deux à deux alors  $b_1, b_2, \dots, b_n$  commutent deux à deux.

– **Si  $n = 2$  :**

Alors  $k = 1$ , par suite on a

$$\star_{i=1}^n a_i = \star_{i=1}^2 a_i = a_1 \star a_2 = a_2 \star a_1 = a_n \star a_k = b_k \star b_n = b_1 \star b_2 = \star_{i=1}^2 b_i = \star_{i=1}^n b_i.$$

– Si  $n \geq 3$  et  $k = 1$  :

$$\begin{aligned}\star_{i=1}^n a_i &= a_1 \star \left( \star_{i=2}^{n-1} a_i \right) \star a_n = a_n \star a_1 \star \left( \star_{i=2}^{n-1} a_i \right) = a_1 \star a_n \star \left( \star_{i=2}^{n-1} a_i \right) \\ &= a_n \star \left( \star_{i=2}^{n-1} a_i \right) \star a_1 = a_n \star \left( \star_{i=2}^{n-1} a_i \right) \star a_k = b_1 \star \left( \star_{i=2}^{n-1} b_i \right) \star b_n \\ &= \star_{i=1}^n b_i.\end{aligned}$$

– Si  $n \geq 3$  et  $k = n - 1$  :

$$\begin{aligned}\star_{i=1}^n a_i &= \left( \star_{i=1}^{n-2} a_i \right) \star a_{n-1} \star a_n = \left( \star_{i=1}^{n-2} a_i \right) \star a_n \star a_{n-1} = \left( \star_{i=1}^{n-2} a_i \right) \star a_n \star a_k \\ &= \left( \star_{i=1}^{n-2} b_i \right) \star b_k \star b_n = \left( \star_{i=1}^{n-2} b_i \right) \star b_{n-1} \star b_n \\ &= \star_{i=1}^n b_i.\end{aligned}$$

– Si  $n \geq 3$  et  $1 < k < n - 1$  :

Alors :  $2 \leq k \leq n - 2 \Rightarrow 2 \leq n - 2 \Rightarrow n \geq 4$ .

$$\begin{aligned}\star_{i=1}^n a_i &= \left( \star_{i=1}^{k-1} a_i \right) \star a_k \star \left( \star_{i=k+1}^{n-1} a_i \right) \star a_n = \left( \star_{i=1}^{k-1} a_i \right) \star \left( \star_{i=k+1}^{n-1} a_i \right) \star a_k \star a_n \\ &= \left( \star_{i=1}^{k-1} a_i \right) \star \left( \star_{i=k+1}^{n-1} a_i \right) \star a_n \star a_k = \left( \star_{i=1}^{k-1} b_i \right) \star \left( \star_{i=k+1}^{n-1} b_i \right) \star b_k \star b_n \\ &= \left( \star_{i=1}^{k-1} b_i \right) \star b_k \star \left( \star_{i=k+1}^{n-1} b_i \right) \star b_n \\ &= \star_{i=1}^n b_i.\end{aligned}$$

### Théorème 1-3-17 :

Soit  $(E, \star)$  un ensemble muni d'une loi de composition interne  $\star$  associative.

Pour tout entier naturel non nul  $n$ , si  $a_1, \dots, a_n$  sont des éléments de  $E$  qui commutent deux à deux et si  $\sigma$  est une permutation de l'ensemble  $I_n = \{1, \dots, n\}$  alors :

$a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux et on a :  $\star_{i=1}^n a_i = \star_{i=1}^n a_{\sigma(i)}$ .

**En particulier :**

– Si la loi  $\star$  est notée multiplicativement,  $n$  est un entier naturel non nul,  $a_1, \dots, a_n$  sont des éléments de  $E$  qui commutent deux à deux et  $\sigma$  est une permutation de l'ensemble  $I_n = \{1, \dots, n\}$  alors,  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux et on a :

$$\prod_{i=1}^n a_i = \prod_{i=1}^n a_{\sigma(i)}.$$

– Si la loi  $\star$  est notée additivement,  $n$  est un entier naturel non nul,  $a_1, \dots, a_n$  sont des éléments de  $E$  qui commutent deux à deux et  $\sigma$  est une permutation de l'ensemble  $I_n = \{1, \dots, n\}$  alors,  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux et on a :

$$\sum_{i=1}^n a_i = \sum_{i=1}^n a_{\sigma(i)}.$$

### Démonstration :

Pour tout entier naturel non nul  $n$ , on pose  $I_n = \{1, 2, \dots, n\}$ .

Montrons par récurrence que pour tout entier naturel non nul  $n$ , si  $a_1, \dots, a_n$  sont des éléments de  $E$  qui commutent deux à deux et si  $\sigma$  est une permutation de l'ensemble  $I_n = \{1, 2, \dots, n\}$  alors,  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux et on a :

$$\star_{i=1}^n a_i = \star_{i=1}^n a_{\sigma(i)}.$$

– **Pour  $n = 1$  :**

Soient  $a_1, \dots, a_n$  des éléments de  $E$  qui commutent deux à deux et  $\sigma$  une permutation de l'ensemble  $I_n$ .

Puisque  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  sont les éléments  $a_1, \dots, a_n$  et puisque  $a_1, \dots, a_n$  commutent deux à deux alors  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux.

$$n = 1 \Rightarrow I_n = I_1 = \{1\} \Rightarrow \sigma(1) = 1.$$

$$\text{Alors : } \star_{i=1}^n a_i = \star_{i=1}^1 a_i = a_1 = a_{\sigma(1)} = \star_{i=1}^n a_{\sigma(i)}.$$

– **Pour  $n - 1$  :**

Supposons que si  $a_1, \dots, a_{n-1}$  sont des éléments de  $E$  qui commutent deux à deux et si  $\sigma$  est une permutation de l'ensemble  $I_{n-1} = \{1, \dots, n-1\}$  alors,  $a_{\sigma(1)}, \dots, a_{\sigma(n-1)}$  commutent deux à deux et on a :  $\star_{i=1}^{n-1} a_i = \star_{i=1}^{n-1} a_{\sigma(i)}$ .

– **Pour  $n$  :**

Montrons qu'alors si  $a_1, \dots, a_n$  sont des éléments de  $E$  qui commutent deux à deux et si  $\sigma$  est une permutation de l'ensemble  $I_n = \{1, 2, \dots, n\}$  alors,  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux et on a :  $\star_{i=1}^n a_i = \star_{i=1}^n a_{\sigma(i)}$ .

Soit  $\sigma$  une permutation de l'ensemble  $I_n$ .

• **Si  $\sigma(n) = n$  :**

Soit  $\sigma'$  la restriction de  $\sigma$  à  $I_{n-1}$ .

Puisque  $\sigma(n) = n$  alors  $\sigma'$  est une permutation de l'ensemble  $I_{n-1}$ .

Soient  $a_1, \dots, a_n$  des éléments quelconques de  $E$  qui commutent deux à deux.

Puisque  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  sont les éléments  $a_1, \dots, a_n$  et puisque  $a_1, \dots, a_n$

commutent deux à deux alors  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux.

D'après l'hypothèse de récurrence on a :  $\star_{i=1}^{n-1} a_i = \star_{i=1}^{n-1} a_{\sigma'(i)} = \star_{i=1}^{n-1} a_{\sigma(i)}$ .

Par suite :  $\star_{i=1}^n a_i = (\star_{i=1}^{n-1} a_i) \star a_n = (\star_{i=1}^{n-1} a_{\sigma(i)}) \star a_{\sigma(n)} = \star_{i=1}^n a_{\sigma(i)}$ .

• **Si  $\sigma(n) \neq n$  :**

Soient  $a_1, \dots, a_n$  des éléments quelconques de  $E$  qui commutent deux à deux.

Puisque  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  sont les éléments  $a_1, \dots, a_n$  et puisque  $a_1, \dots, a_n$

commutent deux à deux alors  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  commutent deux à deux.

Posons  $\sigma(a_n) = k$ ,  $k = \sigma(a_n) \neq n \Rightarrow [n \geq 2 \quad \text{et} \quad k \in I_{n-1}]$ .

Pour tout entier naturel  $i \in I_n$ , posons : 
$$\begin{cases} b_i = a_i & \text{si } i \neq n \text{ et } i \neq k \\ b_n = a_k & \text{si } i = n \\ b_k = a_n & \text{si } i = k \end{cases} .$$

D'après le lemme 1-3-16, on a :  $\star_{i=1}^n a_i = \star_{i=1}^n b_i$ .

Soit  $\tau$  l'application de  $I_n$  vers  $I_n$  définie par :  $\tau : I_n \rightarrow I_n$

$$\begin{aligned} i &\mapsto \tau(i) = i \quad \text{si } i \neq n \text{ et } i \neq k \\ n &\mapsto \tau(n) = k \\ k &\mapsto \tau(k) = i. \end{aligned}$$

• Montrons que  $\tau$  est une permutation de l'ensemble  $I_n$ .

$$\forall i \in I_n : \begin{cases} (\tau \circ \tau)(i) = \tau(\tau(i)) = \tau(i) = i = id_{I_n}(i) & \text{si } i \neq n \text{ et } i \neq k \\ (\tau \circ \tau)(i) = \tau(\tau(n)) = \tau(k) = n = i = id_{I_n}(i) & \text{si } i = n \\ (\tau \circ \tau)(i) = \tau(\tau(k)) = \tau(n) = k = i = id_{I_n}(i) & \text{si } i = k \end{cases} .$$

Alors  $\tau \circ \tau = id_{I_n}$ . Donc  $\tau$  est bijective.

Ce qui prouve que  $\tau$  est une permutation de l'ensemble  $I_n$ .

• Montrons que  $(\tau \circ \sigma)(n) = n$ .

$$(\tau \circ \sigma)(n) = \tau(\sigma(n)) = \tau(k) = n.$$

• Puisque  $(\tau \circ \sigma)(n) = n$ , alors :  $\star_{i=1}^n a_i = \star_{i=1}^n b_i = \star_{i=1}^n b_{(\tau \circ \sigma)(i)} = \star_{i=1}^n b_{\tau(\sigma(i))}$ .

$$\forall i \in I_n : \begin{cases} b_{\tau(\sigma(i))} = b_{\sigma(i)} = a_{\sigma(i)} & \text{si } \sigma(i) \neq n \text{ et } \sigma(i) \neq k \\ b_{\tau(\sigma(i))} = b_{\tau(n)} = b_k = a_n = a_{\sigma(i)} & \text{si } \sigma(i) = n \\ b_{\tau(\sigma(i))} = b_{\tau(k)} = b_n = a_k = a_{\sigma(i)} & \text{si } \sigma(i) = k \end{cases} .$$

$$\text{Alors : } \star_{i=1}^n a_i = \star_{i=1}^n b_{\tau(\sigma(i))} = \star_{i=1}^n a_{\sigma(i)} .$$

**Lemma 1-3-18 :**

Soient  $A$  un ensemble fini non vide et  $a_1, \dots, a_n, b_1, \dots, b_n$  des éléments de  $A$ .  
 Si  $a_1, \dots, a_n$  sont distincts deux à deux,  $b_1, \dots, b_n$  sont distincts deux à deux et  
 $A = \{a_1, \dots, a_n\} = \{b_1, \dots, b_n\}$  alors il existe une permutation  $\sigma$  de l'ensemble  
 $I = \{1, \dots, n\}$  telle que :  $\forall i \in I : b_i = a_{\sigma(i)}$ .

**Démonstration :**

Soient  $u$  et  $v$  les bijections de  $I$  vers  $A$  définies par :

$$\begin{array}{ccc} u : I \rightarrow A & & v : I \rightarrow A \\ i \mapsto u(i) = a_i & \text{et} & i \mapsto v(i) = b_i \end{array} .$$

Puisque  $u$  et  $v$  des bijections de  $I$  vers  $A$ , alors  $\sigma = u^{-1} \circ v$  est une bijection de  $I$  vers  $A$ .  
 Alors  $\sigma$  est une permutation de l'ensemble  $I$  et on a pour tout entier naturel  $i \in I$  :  
 $b_i = id_A(b_i) = (u \circ u^{-1})(b_i) = u(u^{-1}(b_i)) = u(u^{-1}(v(i))) = u((u^{-1} \circ v)(i)) = u(\sigma(i)) = a_{\sigma(i)}$ .

**Théorème et notation 1-3-19 :**

Soient  $(E, \star)$  un ensemble muni d'une loi de composition interne  $\star$  associative,  $I$  un ensemble fini non vide et  $(a_i)_{i \in I}$  une famille d'éléments de  $E$  indexée par  $I$  qui commutent deux à deux (c'est à dire,  $\forall i, j \in I : a_i \star a_j = a_j \star a_i$ ).

Si  $i_1, \dots, i_n$  sont des éléments quelconques de  $I$  distincts deux à deux,  $j_1, \dots, j_n$  sont des éléments quelconques de  $I$  distincts deux à deux et  $I = \{i_1, \dots, i_n\} = \{j_1, \dots, j_n\}$  alors :  $\star_{k=1}^n a_{i_k} = \star_{k=1}^n a_{j_k}$  qui est noté  $\star_{i \in I} a_i$ .

C'est à dire si  $i_1, \dots, i_n$  sont des éléments quelconques de  $I$  distincts deux à deux et si  $I = \{i_1, \dots, i_n\}$  alors :  $\star_{i \in I} a_i = \star_{k=1}^n a_{i_k}$ .

**En particulier :**

- Si la loi  $\star$  est notée multiplicativement, les éléments de la famille  $(a_i)_{i \in I}$  commutent deux à deux (c'est à dire,  $\forall i, j \in I : a_i a_j = a_j a_i$ ),  $i_1, \dots, i_n$  sont des éléments quelconques de  $I$ , distincts deux à deux et  $I = \{i_1, \dots, i_n\}$  alors :  $\prod_{i \in I} a_i = \prod_{k=1}^n a_{i_k}$ .
- Si la loi  $\star$  est notée additivement, les éléments de la famille  $(a_i)_{i \in I}$  commutent deux à deux (c'est à dire,  $\forall i, j \in I : a_i + a_j = a_j + a_i$ ),  $i_1, \dots, i_n$  sont des éléments quelconques de  $I$ , distincts deux à deux et  $I = \{i_1, \dots, i_n\}$  alors :  $\sum_{i \in I} a_i = \sum_{k=1}^n a_{i_k}$ .

**Démonstration :**

Soient  $i_1, \dots, i_n$  des éléments quelconques de  $I$  distincts deux à deux et  $j_1, \dots, j_n$  des éléments quelconques de  $I$  distincts deux à deux tels que  $I = \{i_1, \dots, i_n\} = \{j_1, \dots, j_n\}$ .  
 D'après le lemme 1-3-18, il existe une permutation  $\sigma$  de l'ensemble  $\{1, \dots, n\}$  telle que :  
 $\forall k = 1, \dots, n : j_k = i_{\sigma(k)}$ .

Pour tout entier naturel  $k = 1, \dots, n$ , posons  $x_k = a_{i_k}$ .

D'après le théorème 1-3-17 on a alors :

$$\star_{k=1}^n a_{i_k} = \star_{k=1}^n x_k = \star_{k=1}^n x_{\sigma(k)} = \star_{k=1}^n a_{i_{\sigma(k)}} = \star_{k=1}^n a_{j_k} .$$



**Théorème et notation 1-3-20 :**

Soient  $(E, \star)$  un ensemble muni d'une loi de composition interne  $\star$  associative, et  $A$  un ensemble fini non vide dont les éléments commutent deux à deux (c'est à dire:

$$\forall a, b \in A : a \star b = b \star a).$$

Si  $a_1, \dots, a_n$  sont des éléments quelconques de  $A$  distincts deux à deux,  $b_1, \dots, b_n$  sont des éléments quelconques de  $A$  distincts deux à deux et  $A = \{a_1, \dots, a_n\} = \{b_1, \dots, b_n\}$ , alors :  $\star_{i=1}^n a_i = \star_{i=1}^n b_i$  qui est noté  $\star_{a \in A} a$ .

C'est à dire si  $a_1, \dots, a_n$  sont des éléments quelconques de  $A$  distincts deux à deux et si  $A = \{a_1, \dots, a_n\}$  alors :  $\star_{a \in A} a = \star_{i=1}^n a_i$ .

**En particulier :**

- Si la loi  $\star$  est notée multiplicativement,  $a_1, \dots, a_n$  sont des éléments quelconques de  $A$  distincts deux à deux et  $A = \{a_1, \dots, a_n\}$ , alors :  $\prod_{a \in A} a_i = \prod_{i=1}^n a_i$ .
- Si la loi  $\star$  est notée additivement,  $a_1, \dots, a_n$  sont des éléments quelconques de  $A$  distincts deux à deux et  $A = \{a_1, \dots, a_n\}$ , alors :  $\sum_{i \in I} a_i = \sum_{i=1}^n a_i$ .

**Démonstration :**

Soient  $a_1, \dots, a_n$  des éléments quelconques de  $A$  distincts deux à deux et  $b_1, \dots, b_n$  des éléments quelconques de  $A$  distincts deux à deux tels que

$$A = \{a_1, \dots, a_n\} = \{b_1, \dots, b_n\}.$$

D'après le lemme 1-3-18, il existe une permutation  $\sigma$  de l'ensemble  $\{1, \dots, n\}$  telle que :

$$\forall i = 1, \dots, n : b_i = a_{\sigma(i)}$$

D'après le théorème 1-3-17 on a alors :

$$\star_{i=1}^n a_i = \star_{i=1}^n a_{\sigma(i)} = \star_{i=1}^n b_i.$$

**Corollaire 1-3-21 :**

Soient  $E$  et  $F$  deux ensembles munis respectivement des lois de composition internes  $\star$  et  $T$  associatives,  $I$  un ensemble fini non vide et  $(a_i)_{i \in I}$  une famille d'éléments de  $E$  indexée par  $I$  qui commutent deux à deux (c'est à dire,  $\forall i, j \in I : a_i \star a_j = a_j \star a_i$ ).

Si  $f$  est un homomorphisme de  $(E, \star)$  vers  $(F, T)$  alors, les éléments de la famille  $(f(a_i))_{i \in I}$  commutent deux à deux (c'est à dire,  $\forall i, j \in I : f(a_i) T f(a_j) = f(a_j) T f(a_i)$ )

et on a :  $f(\star_{i \in I} a_i) = T_{i \in I} f(a_i)$ .

**En particulier :**

- Si les lois  $\star$  et  $T$  sont notées multiplicativement alors, les éléments de la famille  $(f(a_i))_{i \in I}$  commutent deux à deux (c'est à dire,  $\forall i, j \in I : f(a_i) f(a_j) = f(a_j) f(a_i)$ ) et on a :  $f\left(\prod_{i \in I} a_i\right) = \prod_{i \in I} f(a_i)$ .
- Si les lois  $\star$  et  $T$  sont notées additivement alors, les éléments de la famille  $(f(a_i))_{i \in I}$  commutent deux à deux (c'est à dire,  $\forall i, j \in I : f(a_i) + f(a_j) = f(a_j) + f(a_i)$ ) et on a :  $f\left(\sum_{i \in I} a_i\right) = \sum_{i \in I} f(a_i)$ .

- Si la loi  $\star$  est notée multiplicativement et la loi  $T$  est notée additivement alors, les éléments de la famille  $(f(a_i))_{i \in I}$  commutent deux à deux (c'est à dire,  $\forall i, j \in I$  :

$$f(a_i) + f(a_j) = f(a_j) + f(a_i) \text{ et on a : } f\left(\prod_{i \in I} a_i\right) = \sum_{i \in I} f(a_i).$$

- Si la loi  $\star$  est notée additivement et la loi  $T$  est notée multiplicativement alors, les éléments de la famille  $(f(a_i))_{i \in I}$  commutent deux à deux (c'est à dire,  $\forall i, j \in I$  :

$$f(a_i)f(a_j) = f(a_j)f(a_i) \text{ et on a : } f\left(\sum_{i \in I} a_i\right) = \prod_{i \in I} f(a_i).$$

### Démonstration :

Soit  $f$  un homomorphisme de  $(E, \star)$  vers  $(F, T)$ .

- $\forall i, j \in I : f(a_i)Tf(a_j) = f(a_i \star a_j) = f(a_j \star a_i) = f(a_j)Tf(a_i)$ .

Donc les éléments de la famille  $(f(a_i))_{i \in I}$  commutent deux à deux.

- Soient  $i_1, \dots, i_n$  les éléments de  $I$  distincts deux à deux.

Puise  $I = \{i_1, \dots, i_n\}$  et puisque les éléments de la famille  $(a_i)_{i \in I}$  commutent deux à deux alors (d'après la notation 1-3-19),  $\star_{i \in I} a_i = \star_{k=1}^n a_{i_k}$ .

Puise  $I = \{i_1, \dots, i_n\}$  et puisque les éléments de la famille  $(f(a_i))_{i \in I}$  commutent deux à deux alors (d'après la notation 1-3-19),  $T_{i \in I} f(a_i) = T_{k=1}^n f(a_{i_k})$ .

Par suite on a :  $f(\star_{i \in I} a_i) = f(\star_{k=1}^n a_{i_k}) = T^n_{k=1} f(a_{i_k}) = T_{i \in I} f(a_i)$ .

### Corollaire 1-3-22 :

Soient  $E$  et  $F$  deux ensembles munis respectivement des lois de composition internes  $\star$  et  $T$  associatives, et  $A$  un ensemble fini non vide dont les éléments commutent deux à deux (c'est à dire:  $\forall a, b \in A : a \star b = b \star a$ ).

Si  $f$  est un homomorphisme de  $(E, \star)$  vers  $(F, T)$  alors, les éléments de l'ensemble  $f(A)$  commutent deux à deux (c'est à dire,  $\forall a, b \in A : f(a)Tf(b) = f(b)Tf(a)$ ) et on a :

$$f(\star_{a \in A} a) = T_{a \in A} f(a).$$

#### En particulier :

- Si les lois  $\star$  et  $T$  sont notées multiplicativement alors, les éléments de l'ensemble  $f(A)$  commutent deux à deux (c'est à dire,  $\forall a, b \in A : f(a)f(b) = f(b)f(a)$ ) et on a :

$$f\left(\prod_{a \in A} a\right) = \prod_{a \in A} f(a).$$

- Si les lois  $\star$  et  $T$  sont notées additivement alors, les éléments de l'ensemble  $f(A)$  commutent deux à deux (c'est à dire,  $\forall a, b \in A : f(a) + f(b) = f(b) + f(a)$ ) et on a :

$$f\left(\sum_{a \in A} a\right) = \sum_{a \in A} f(a).$$

- Si la loi  $\star$  est notée multiplicativement et la loi  $T$  est notée additivement alors, les éléments de l'ensemble  $f(A)$  commutent deux à deux (c'est à dire,  $\forall a, b \in A$  :

$$f(a) + f(b) = f(b) + f(a) \text{ et on a : } f\left(\prod_{a \in A} a\right) = \sum_{a \in A} f(a).$$

- Si la loi  $\star$  est notée additivement et la loi  $T$  est notée multiplicativement alors, les éléments de l'ensemble  $f(A)$  commutent deux à deux (c'est à dire,  $\forall a, b \in A$  :

$$f(a)f(b) = f(b)f(a) \text{ et on a : } f\left(\sum_{a \in A} a\right) = \prod_{a \in A} f(a).$$

**Démonstration :**

Soit  $f$  un homomorphisme de  $(E, \star)$  vers  $(F, T)$ .

- $\forall a, b \in A : f(a)Tf(b) = f(a \star b) = f(b \star a) = f(b)Tf(a)$ .  
Donc les éléments de l'ensemble  $f(A)$  commutent deux à deux.
- Soient  $a_1, \dots, a_n$  les éléments de  $A$  distincts deux à deux.  
Puisque  $A = \{a_1, \dots, a_n\}$  et puisque les éléments de l'ensemble  $f(A)$  commutent deux à deux alors (d'après la notation 1-3-20),  $\star_{a \in A} a = \star_{i=1}^n a_i$ .  
Puisque  $A = \{a_1, \dots, a_n\}$  et puisque les éléments de la famille  $(f(a))_{a \in A}$  commutent deux à deux alors (d'après la notation 1-3-19),  $T_{a \in A} f(a_i) = T_{i=1}^n f(a_i)$ .  
Par suite on a :  $f(\star_{a \in A} a) = f(\star_{i=1}^n a_i) = T_{i=1}^n f(a_i) = T_{a \in A} f(a)$ .

**Corollaire 1-3-23 :**

Soient  $E$  et  $F$  deux ensembles munis respectivement des lois de composition internes  $\star$  et  $T$  associatives,  $A$  un ensemble fini non vide dont les éléments commutent deux à deux (c'est à dire:  $\forall a, b \in A : a \star b = b \star a$ ) et  $f$  un homomorphisme de  $(E, \star)$  vers  $(F, T)$ .

Si la restriction de  $f$  à  $A$  est injective (en particulier si  $f$  est injectif), alors :

$$f(\star_{a \in A} a) = T_{b \in f(A)} b.$$

**En particulier :**

- Si les lois  $\star$  et  $T$  sont notées multiplicativement et si la restriction de  $f$  à  $A$  est injective (en particulier si  $f$  est injectif), alors :  $f\left(\prod_{a \in A} a\right) = \prod_{b \in f(A)} b$ .
- Si les lois  $\star$  et  $T$  sont notées additivement et si la restriction de  $f$  à  $A$  est injective (en particulier si  $f$  est injectif), alors :  $f\left(\sum_{a \in A} a\right) = \sum_{b \in f(A)} b$ .
- Si la loi  $\star$  est notée multiplicativement, la loi  $T$  est notée additivement et la restriction de  $f$  à  $A$  est injective (en particulier si  $f$  est injectif), alors :  $f\left(\prod_{a \in A} a\right) = \sum_{b \in f(A)} b$ .
- Si la loi  $\star$  est notée additivement et la loi  $T$  est notée multiplicativement et la restriction de  $f$  à  $A$  est injective (en particulier si  $f$  est injectif), alors :

$$f\left(\sum_{a \in A} a\right) = \prod_{b \in f(A)} b.$$

**Démonstration :**

Supposons que la restriction de  $f$  à  $A$  est injective.

Soient  $a_1, \dots, a_n$  les éléments de  $A$  distincts deux à deux.

Puisque  $A = \{a_1, \dots, a_n\}$  et puisque la restriction de  $f$  à  $A$  est injective alors,  $f(a_1), \dots, f(a_n)$  sont distincts deux à deux et  $f(A) = \{f(a_1), \dots, f(a_n)\}$ .

On a donc :

$$\begin{aligned} f(\star_{a \in A} a) &= f(\star_{i=1}^n a_i) \text{ (d'après la notation 1-3-20)} \\ &= T_{i=1}^n f(a_i) \\ &= T_{b \in f(A)} b. \text{ (d'après la notation 1-3-5, car } f(A) = \{f(a_1), \dots, f(a_n)\} \text{).} \end{aligned}$$

## 2 - Groupes :

### 2-1-Généralités :

#### Définition 2-1-1 :

Soit  $(G, \star)$  un ensemble muni d'une loi de composition interne. On dit que  $(G, \star)$  est un groupe ou  $G$  est groupe pour la loi  $\star$  ou  $G$  est groupe si :

i) la loi  $\star$  est associative, c'est à dire si on a :

$$\forall x, y, z \in G : (x \star y) \star z = x \star (y \star z)$$

ii)  $G$  admet un élément neutre  $e$  pour la loi  $\star$ , c'est à dire si :

$$\exists e \in G \quad tq : \forall x \in G : x \star e = e \star x = x.$$

iii) tout élément de  $G$  admet un symétrique pour la loi  $\star$ , c'est à dire si :

$$\forall x \in G : \exists x' \in G \quad tq : x \star x' = x' \star x = e.$$

#### Dans ce cas :

- Si la loi  $\star$  est abélien on dit que le groupe est abélien ou commutatif.
- Si la loi  $\star$  est notée multiplicativement on dit que le groupe est multiplicatif.
- Si la loi  $\star$  est notée additivement on dit que le groupe est additif.
- Si  $G$  est fini on dit que le groupe est d'ordre fini et dans ce le cardinale  $|G|$  est appelé l'ordre de  $G$ .
- Si  $X$  est une partie de  $G$ , l'ensemble des symétriques des éléments de  $X$  est noté  $X'$ .
- Si  $G$  est multiplicatif et si  $X$  est une partie de  $G$ , l'ensemble des inverses des éléments de  $X$  est noté  $X^{-1}$ .  
C'est à dire si  $G$  est multiplicatif et si  $X$  est une partie de  $G$ ,  $X^{-1} = \{x^{-1} \quad tq : x \in X\}$ .
- Si  $G$  est additif et si  $X$  est une partie de  $G$ , l'ensemble des opposés des éléments de  $X$  est noté  $-X$ .  
C'est à dire si  $G$  est additif et si  $X$  est une partie de  $G$ ,  $-X = \{-x \quad tq : x \in X\}$ .
- Si  $G$  est infini on dit que le groupe est d'ordre infini.
- Les groupes sont en générales multiplicatifs .
- Les groupes abéliens sont par fois additifs.

#### Exemple 2-1-2 :

- \*  $(\mathbb{N}, +), (\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$  ne sont pas des groupes.
- \*  $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot), (\mathbb{Q}^{*+}, \cdot), (\mathbb{R}^{*+}, \cdot)$  sont des groupes abéliens.
- \* Soit  $E$  un ensemble quelconque.
  - $(\mathcal{P}(E), \cup)$  et  $(\mathcal{P}(E), \cap)$  ne sont pas des groupes.
  - $(\mathcal{P}(E), \Delta)$  est un groupe abélien.
  - $(S(E), \circ)$  est un groupe appelé le groupe symétrique de  $E$  qui est :
    - abélien si  $E = \emptyset$  ou  $E$  contient un seul élément ou 2 éléments.
    - non abélien si  $E$  contient au moins 3 éléments. $S(E)$  étant l'ensemble des permutations de  $E$ .
- \* Si  $G$  est un groupe alors  $\mathcal{P}(G)$  n'est pas un groupe pour la loi induite.
- \* Si  $G$  et  $H$  sont deux groupes alors  $G \times H$  est un groupe.
- \* Si  $G_1, G_2, \dots, G_n$  sont des groupes alors  $\prod_{i=1}^n G_i = G_1 \times G_2 \times \dots \times G_n$  est un groupe.

- \* Si  $G$  est un groupe alors pour tout entier naturel non nul  $n$ ,  $G^n$  est un groupe.  
**En particulier** : pour tout entier naturel non nul  $n$ ,  $(\mathbb{Z}^n, +)$  est un groupe abélien.
- \* Si  $G$  est un groupe et si  $E$  est un ensemble quelconque alors :  $G^E$  est un groupe.

### Propriétés 2-1-3 :

Soit  $G$  un groupe.

- 1) Tous les éléments de  $G$  sont réguliers pour la loi de  $G$ .
- 2)  $\emptyset$  n'est pas symétrisable pour la loi induite de  $G$  à  $\mathcal{P}(G)$ .
- 3)  $\mathcal{P}(G)$  n'est un groupe pour la loi induite de  $G$  à  $\mathcal{P}(G)$ .
- 4) Si  $X$  est une partie de  $G$  alors  $X$  est symétrisable pour la loi induite de  $G$  à  $\mathcal{P}(G)$  si et seulement si  $X$  est un singleton.
- 5) Si  $X$  est une partie de  $G$  alors  $(X')' = X$  En particulier :
  - si  $G$  est un groupe multiplicatif alors :  $(X^{-1})^{-1} = X$ .
  - si  $G$  est un groupe additif alors :  $-(-X) = X$ .
- 6) Si  $X$  et  $Y$  sont des parties de  $G$  et si la loi de  $G$  est noté  $\star$  alors  $(X \star Y)' = Y' \star X'$ .  
 En particulier :
  - si  $G$  est un groupe multiplicatif alors :  $(XY)^{-1} = Y^{-1}X^{-1}$ .
  - si  $G$  est un groupe additif alors :  $-(X + Y) = -Y - X$ .
- 7) Si  $G$  est un groupe multiplicatif alors pour tout élément  $a$  de  $G$  l'application suivante :

$$f: \mathbb{Z} \rightarrow G$$

$$n \mapsto f(n) = a^n$$

est un homomorphisme de  $(\mathbb{Z}, +)$  vers  $(G, \cdot)$ .

- 8) Si  $G$  est un groupe additif alors pour tout élément  $a \in G$  l'application suivante :

$$f: \mathbb{Z} \rightarrow G$$

$$n \mapsto f(n) = na$$

est un homomorphisme de  $(\mathbb{Z}, +)$  vers  $(G, +)$ .

- 9) Soient  $H$  un autre groupe,  $f$  un homomorphisme de  $G$  vers  $H$ .  
 Si  $e$  est l'élément neutre de  $G$  et si  $\varepsilon$  est l'élément neutre de  $H$  alors :
  - a)  $f(e) = \varepsilon$  c'est à dire :  $e \in \ker f$ .
  - b) Si  $a$  est un élément de  $G$ ,  $a'$  est le symétrique de  $a$  et  $f(a)'$  est le symétrique de  $f(a)$  alors :  $f(a') = f(a)'$ .
  - c)  $f$  est injectif si et seulement si  $\ker f = \{e\}$
- 10) Soient  $H$  un autre groupe,  $f$  un homomorphisme de  $G$  vers  $H$  et  $a \in G$  un élément quelconque de  $G$ .
  - a) Si  $G$  et  $H$  sont multiplicatifs alors :  $\forall n \in \mathbb{Z} : f(a^n) = f(a)^n$ .
  - b) Si  $G$  et  $H$  sont additifs alors :  $\forall n \in \mathbb{Z} : f(na) = nf(a)$ .
  - c) Si  $G$  est multiplicatif et si  $H$  est additif alors :  $\forall n \in \mathbb{Z} : f(a^n) = nf(a)$ .
  - d) Si  $G$  est additif et si  $H$  est multiplicatif alors :  $\forall n \in \mathbb{Z} : f(na) = f(a)^n$ .

### Démonstration :

- 1) Soient  $\star$  la loi composition interne du groupe  $G$  et  $e$  l'élément neutre de  $G$  pour la loi  $\star$ .  
 Soit  $a$  un élément quelconque de  $G$  et  $a'$  son symétrique.

$\forall x, y \in G :$

$$\begin{aligned} a \star x = a \star y &\Rightarrow a' \star (a \star x) = a' \star (a \star y) \Rightarrow (a' \star a) \star x = (a' \star a) \star y \\ &\Rightarrow e \star x = e \star y \\ &\Rightarrow x = y. \\ x \star a = y \star a &\Rightarrow (x \star a) \star a' = (y \star a) \star a' \Rightarrow x \star (a \star a') = y \star (a \star a') \\ &\Rightarrow x \star e = y \star e \\ &\Rightarrow x = y. \end{aligned}$$

Donc  $a$  est un élément régulier de  $G$ .

Ce qui montre que tous les éléments de  $G$  sont réguliers pour la loi de  $G$ .

- 2) Soient  $\star$  la loi composition interne du groupe  $G$  et  $e$  l'élément neutre de  $G$  pour la loi  $\star$ .

Puisque  $\emptyset$  est absorbant alors :  $\forall X \in \mathcal{P}(G) : \emptyset \star X = \emptyset \neq \{e\}$ .

Donc  $\emptyset$  n'est pas symétrisable pour la loi induite de  $G$  à  $\mathcal{P}(G)$ .

- 3) Puisque  $\emptyset$  est un élément de  $\mathcal{P}(G)$  qui n'est pas symétrisable alors  $\mathcal{P}(G)$  n'est un groupe pour la loi induite de  $G$  à  $\mathcal{P}(G)$ .

- 4) Soient  $\star$  la loi composition interne du groupe  $G$ ,  $e$  l'élément neutre de  $G$  pour la loi  $\star$  et  $X$  une partie de  $G$ .

$\Rightarrow$  ) **Si  $X$  est symétrisable :**

Soit  $Y$  le symétrique de  $X$ .

$$X \star Y = \{e\} \neq \emptyset \Rightarrow [X \neq \emptyset \text{ et } Y \neq \emptyset].$$

Soient  $a$  un élément de  $X$  et  $b$  un élément de  $Y$ .

$$a \star b \in X \star Y = \{e\} \Rightarrow a \star b = e. \text{ Donc } b \text{ est symétrique de } a.$$

$$\forall x \in X : x \star b \in X \star Y = \{e\} \Rightarrow x \star b = e = a \star b \Rightarrow x = a.$$

Ce qui montre que  $X = \{a\}$  est un singleton.

$\Leftarrow$  ) **Si  $X$  est un singleton :**

Soient  $a$  l'élément de  $X$  et  $a'$  son symétrique.

$$\begin{cases} X \star \{a'\} = \{a\} \star \{a'\} = \{a \star a'\} = \{e\} \\ \{a'\} \star X = \{a'\} \star \{a\} = \{a' \star a\} = \{e\} \end{cases}.$$

Donc  $X$  est symétrisable pour la loi induite de  $G$  à  $\mathcal{P}(G)$  et son symétrique est égal à  $\{a'\}$ .

- 5) Soient  $\star$  la loi composition interne du groupe  $G$ ,  $e$  l'élément neutre de  $G$  pour la loi  $\star$  et  $X$  une partie de  $G$ .

$\subset$  ) Soit  $x$  un élément quelconque de  $(X')'$ .

Alors il existe un élément  $x'$  de  $X'$  tel que  $x$  soit le symétrique de  $x'$ .

Puisque  $x'$  est un élément de  $X'$  alors il existe un élément  $x''$  de  $X$  tel que  $x'$  soit le symétrique de  $x''$ .

Puisque  $x$  est le symétrique de  $x'$  et  $x'$  soit le symétrique de  $x''$  alors :

$$x = x'' \in X.$$

$$\text{Donc : } (X')' \subset (X')'.$$

$\supset$  ) Soient  $x$  un élément quelconque de  $X$  et  $x'$  son symétrique.

$$\text{Alors } x' \in X'.$$

$$\text{Puisque } x \text{ est le symétrique de } x' \in X' \text{ alors } x \in (X')'.$$

$$\text{Donc : } X \subset (X')'.$$

Ce qui montre que  $(X')' = (X')'$ .

En particulier :

- si  $G$  est un groupe multiplicatif alors :  $(X^{-1})^{-1} = X$ .

- si  $G$  est un groupe additif alors :  $-(-X) = X$ .

6) Soient  $X$  et  $Y$  deux parties de  $G$  et  $\star$  la loi  $G$ .

⊂ ) Soit  $x$  un élément quelconque de  $(X \star Y)'$ .

Alors il existe un élément  $u$  de  $X \star Y$  tel que  $x$  soit le symétrique de  $u$ .

$$u \in X \star Y \Rightarrow [\exists a \in X \text{ et } \exists b \in Y \text{ tq : } u = a + b].$$

Soient  $a'$  le symétrique de  $a$  et  $b'$  le symétrique de  $b$ .

Puisque  $x$  est le symétrique de  $u = a + b$  alors :  $x = b' \star a' \in Y' \star X'$

$$\text{Donc : } (X \star Y)' \subset Y' \star X'$$

⊃ ) Soient  $x$  un élément quelconque de  $Y' \star X'$

Alors il existe un élément  $v$  de  $Y'$  et un élément  $u$  de  $X'$  tel que  $x = v \star u$ .

Puisque  $u \in X'$  et puisque  $v \in Y'$  alors il existe un élément  $a$  de  $X$  et un élément  $b$  de  $Y$  tel que  $u$  soit le symétrique de  $a$  et  $v$  soit le symétrique de  $b$ .

Donc  $x = v \star u$  est le symétrique de  $a \star b \in X \star Y$ . Par suite  $x \in (X \star Y)'$

$$\text{On a alors : } Y' \star X' \subset (X \star Y)'.$$

Ce qui montre que  $(X \star Y)' = Y' \star X'$

En particulier :

- si  $G$  est un groupe multiplicatif alors :  $(XY)^{-1} = Y^{-1}X^{-1}$ .

- si  $G$  est un groupe additif alors :  $-(X + Y) = -Y - X$ .

7) Supposons que  $G$  est un groupe multiplicatif.

Soient  $a$  un élément quelconque de  $G$  et  $f$  l'application suivante :

$$f: \mathbb{Z} \rightarrow G$$

$$n \mapsto f(n) = a^n.$$

$$\forall n, m \in \mathbb{Z} : f(n + m) = a^{n+m} = a^n a^m = f(n)f(m).$$

Donc  $f$  est un homomorphisme de  $(\mathbb{Z}, +)$  vers  $(G, \cdot)$ .

8) Supposons que  $G$  est un groupe additif.

Soient  $a$  un élément quelconque de  $G$  et  $f$  l'application suivante :

$$f: \mathbb{Z} \rightarrow G$$

$$n \mapsto f(n) = na.$$

$$\forall n, m \in \mathbb{Z} : f(n + m) = (n + m)a = na + ma = f(n) + f(m).$$

Donc  $f$  est un homomorphisme de  $(\mathbb{Z}, +)$  vers  $(G, +)$ .

9) Soient  $e$  l'élément neutre de  $G$ ,  $\varepsilon$  l'élément neutre de  $H$ ,  $\star$  la loi du groupe  $G$  et  $T$  la loi du groupe  $H$ .

$$a) f(e)Tf(e) = f(e \star e) = f(e) = f(e)T\varepsilon.$$

D'après 1),  $f(e)$  est un élément régulier de  $H$ . Donc  $f(e) = \varepsilon$ .

Ce qui montre que :  $e \in \ker f$ .

b) Soient  $a$  un élément de  $G$ ,  $a'$  le symétrique de  $a$  et  $f(a)'$  le symétrique de  $f(a)$ .

$$f(a)Tf(a') = f(a \star a') = f(e) = \varepsilon = f(a)Tf(a)' \Rightarrow f(a') = f(a)'.$$

c)  $\Rightarrow$  ) **Si  $f$  est injectif :**

$$e \in \ker f \Rightarrow \{e\} \subset \ker f.$$

$$\forall a \in \ker f : f(a) = \varepsilon = f(e) \Rightarrow a = e \in \{e\}. \text{ Donc : } \ker f \subset \{e\}.$$

$$\text{Ce qui montre que } \ker f = \{e\}$$

$\Leftarrow$  ) **Si  $\ker f = \{e\}$  :**

Soient  $a$  et  $b$  deux éléments quelconques de  $G$  tels que  $f(a) = f(b)$ .

Posons  $b'$  le symétrique de  $b$ ,  $f(b)'$  le symétrique de  $f(b)$  et  $f(a)'$

le symétrique de  $f(a)$ .

$$f(a \star b') = f(a)Tf(b') = f(a)Tf(b)' = f(a)Tf(a)' = \varepsilon \Rightarrow a \star b' \in \ker f = \{e\}.$$

Donc :

$$a \star b' = e \Rightarrow (a \star b') \star b = e \star b \Rightarrow a \star (b' \star b) = b \Rightarrow a \star e = b \Rightarrow a = b.$$

Ce qui montre que  $f$  est injectif.

10) a) Supposons que  $G$  et  $H$  sont multiplicatifs. et soit  $n$  un entier relatif quelconque.

- **Si  $n > 0$  :**

D'après la propriété 1-3-9 b),  $f(a^n) = f(a)^n$ .

- **Si  $n = 0$  :**

Soient  $e$  l'élément neutre de  $G$  et  $\varepsilon$  l'élément neutre de  $H$ .

$$f(a^n) = f(a^0) = f(e) = \varepsilon = f(a)^0 = f(a)^n.$$

- **Si  $n < 0$  :**

$$f(a^n) = f((a^{-1})^{-n}) = f(a^{-1})^{-n} = (f(a)^{-1})^{-n} = f(a)^n.$$

b) Supposons que  $G$  et  $H$  sont additifs. et soit  $n$  un entier relatif quelconque.

- **Si  $n > 0$  :**

D'après la propriété 1-3-9 c),  $f(na) = nf(a)$ .

- **Si  $n = 0$  :**

$$f(a^n) = f(0a) = f(0_G) = 0_H = 0f(a) = nf(a).$$

- **Si  $n < 0$  :**

$$f(na) = f((-n)(-a)) = (-n)f(-a) = (-n)[-f(a)] = nf(a).$$

c) Supposons que  $G$  est multiplicatif et  $H$  est additif.

Soit  $n$  un entier relatif quelconque.

- **Si  $n > 0$  :**

D'après la propriété 1-3-9 d),  $f(a^n) = nf(a)$ .

- **Si  $n = 0$  :**

Soient  $e$  l'élément neutre de  $G$ .

$$f(a^n) = f(a^0) = f(e) = 0_H = 0f(a) = nf(a).$$

- **Si  $n < 0$  :**

$$f(a^n) = f((a^{-1})^{-n}) = (-n)f(a^{-1}) = (-n)[-f(a)] = nf(a).$$

d) Supposons que  $G$  est additif et  $H$  est multiplicatif.

Soit  $n$  un entier relatif quelconque.

- **Si  $n > 0$  :**

D'après la propriété 1-3-9 d),  $f(na) = f(a)^n$ .

- **Si  $n = 0$  :**

Soient  $\varepsilon$  l'élément neutre de  $H$ .

$$f(na) = f(0a) = f(0_G) = \varepsilon = f(a)^0 = f(a)^n.$$

- **Si  $n < 0$  :**

$$f(na) = f((-n)(-a)) = f(-a)^{-n} = (f(a)^{-1})^{-n} = f(a)^n.$$

## 2-2 - Sous-groupes :

### Définition 2-2-1 :

Soient  $G$  un groupe et  $H$  une partie de  $G$ .

On dit que  $H$  est un sous-groupe de  $G$  et on note  $H$  est un s.g de  $G$  si on a les deux propriétés suivantes :

- i)  $H$  est stable pour la loi de  $G$ .
- ii)  $H$  est un groupe pour la restriction de la loi de  $G$  à  $H$ .



**Remarque 2-2-2 :**

Soient  $G$  un groupe et  $H$  une partie de  $G$ .

- 1) Si  $H$  est un sous-groupe de  $G$  alors :
  - a)  $H$  et  $G$  contiennent le même élément neutre.
  - b) Le symétrique d'un élément quelconque  $x$  de  $H$  dans  $H$  est égal au symétrique de  $x$  dans  $G$ .
- 2) Si  $H$  ne contient pas l'élément neutre de  $G$  alors  $H$  n'est pas un sous-groupe de  $G$ .

**Démonstration :**

Notons par  $\star$  la loi de  $G$  et par  $e$  l'élément neutre de  $G$ .

- 1) a) Soit  $e'$  l'élément neutre de  $H$ .

$$e' \star e' = e' = e' \star e \Rightarrow e' = e \text{ (car } e' \text{ est régulier).}$$

Donc  $H$  et  $G$  contiennent le même élément neutre.

- b) Soient  $x$  un élément quelconque de  $H$ ,  $x'$  son symétrique dans  $G$  et  $x''$  son symétrique dans  $H$ .

$$x'' = x'' \star e = x'' \star (x \star x') = (x'' \star x) \star x' = e \star x' = x'.$$

Donc le symétrique d'un élément quelconque  $x$  de  $H$  dans  $H$  est égal au symétrique de  $x$  dans  $G$ .

- 2) Si  $H$  ne contient pas l'élément neutre de  $G$  alors (d'après 1) a))  $H$  n'est pas un sous-groupe de  $G$ .

**Propriétés caractéristiques 2-2-3 :**

Soient  $(G, \star)$  un groupe,  $e$  l'élément neutre de  $G$  et  $H$  une partie.

- 1) Pour que  $H$  soit un sous-groupe de  $G$  il faut et il suffit qu'on a les trois propriétés suivantes :
  - i)  $H \neq \emptyset$
  - ii)  $H$  est stable pour la loi de  $G$  (c'est à dire :  $\forall x, y \in H : x \star y \in H$ )
  - iii)  $\forall x \in H : x' \in H$  (où  $x'$  est le symétrique de  $x$  dans  $G$ ).
- 2) Pour que  $H$  soit un sous-groupe de  $G$  il faut et il suffit qu'on a les deux propriétés suivantes :
  - i)  $H \neq \emptyset$
  - ii)  $\forall x, y \in H : x \star y' \in H$  (où  $y'$  est le symétrique de  $y$  dans  $G$ ).

**Démonstration :**

- 1)  $\Rightarrow$  ) **Si  $H$  est un sous-groupe de  $G$  :**

- $e \in H \Rightarrow H \neq \emptyset$ . Donc la propriété i) est vérifiée.
- Puisque  $H$  est un sous-groupe de  $G$  alors  $H$  est stable pour la loi de  $G$ .  
Donc la propriété ii) est vérifiée.
- Soient  $x$  un élément quelconque de  $H$ .  
Puisque  $H$  est un groupe (car  $H$  est un sous-groupe de  $G$ ) alors  $x$  est symétrisable dans  $H$ .

Soit  $x'$  le symétrique de  $x$  dans  $G$ .

D'après la remarque 2-2-2-1) b),  $x'$  est aussi le symétrique de  $x$  dans  $H$ .

Ce qui montre que  $x' \in H$ .

Donc la propriété iii) est vérifiée.

⇐ ) **Si les trois propriétés i), ii) et iii) sont vérifiées :**

- D'après ii)  $H$  est stable pour la loi de  $G$ .

- $\forall x, y, z \in H : x, y, z \in G \Rightarrow (x \star y) \star z = x \star (y \star z)$ .

Donc la restriction de la loi de  $G$  à  $H$  est associative.

- Soient  $a$  un élément de  $H$  ( $a$  existe d'après i)) et  $a'$  son symétrique dans  $G$ .

D'après iii),  $a' \in H$ . Par suite (d'après ii)),  $e = a \star a' \in H$ .

Pour tout élément  $x$  de  $H$ , on a  $x \star e = e \star x = x$ .

Donc  $e$  est l'élément neutre de  $H$ .

- Soient  $x$  un élément quelconque de  $H$  et  $x'$  son symétrique dans  $G$ .

D'après iii),  $x' \in H$ . et on a :  $x \star x' = x' \star x = e$ .

Donc  $x'$  est le symétrique de  $x$  dans  $H$ .

Ce qui montre que  $H$  est un sous-groupe de  $G$ .

2) ⇒ ) **Si  $H$  est un sous-groupe de  $G$  :**

- D'après 1) i),  $e \in H \Rightarrow H \neq \emptyset$ . Donc la propriété 2) i) est vérifiée.

- Soient  $x$  et  $y$  deux éléments quelconques de  $H$ , et soit  $y'$  le symétrique de  $y$  dans  $G$ .

D'après 1) iii)  $y' \in H$ .

D'après 1) ii)  $x \star y' \in H$ .

Donc la propriété 2) i) est vérifiée.

⇐ ) **Si les deux propriétés i) et ii) sont vérifiées :**

- D'après 1) i), la propriété 2) i) est vérifiée.

- Soient  $a$  un élément de  $H$  ( $a$  existe d'après 2) i)) et  $a'$  son symétrique dans  $G$ .

D'après 2) ii),  $e = a \star a' \in H$ . (car  $a, a' \in H$ ).

- Soient  $x$  un élément quelconque de  $H$  et  $x'$  son symétrique dans  $G$ .

$e, x \in H \Rightarrow x' = e \star x' \in H$  (d'après 2) ii)).

Donc la propriété 1) iii) est vérifiée.

- Soient  $x$  et  $y$  deux éléments quelconques de  $H$ , et soit  $y'$  le symétrique de  $y$  dans  $G$ .

D'après la propriété suivantes  $y' \in H$ .

Puisque  $x, y' \in H$  alors (d'après 2) ii)),  $x \star y' \in H$ .

Donc  $H$  est stable pour la loi de  $G$ . Par suite la propriété 2) ii) est vérifiée.

Puisque les propriétés i), ii) et iii) de 1) sont vérifiées, alors  $H$  est un sous-groupe de  $G$ .

### Exemples et propriétés 2-2-4 :

Soient  $G$  un groupe et  $e$  son élément neutre.

1)  $G$  et  $\{e\}$  sont des sous-groupes de  $G$  appelés les sous-groupes triviaux de  $G$ .

2) Si  $H$  et  $K$  sont des sous-groupes de  $G$  alors  $H \cap K$  est un sous-groupe de  $G$ .

3) Si  $E$  est un ensemble non vide de sous-groupes de  $G$  alors l'intersection des éléments de  $G$  est un sous-groupe de  $G$ .

C'est à dire si  $E$  est un ensemble non vide de sous-groupes de  $G$  alors  $\bigcap_{H \in E} H$

est un sous-groupe de  $G$ .

- 4) Si  $I$  est un ensemble non vide et si  $(H_i)_{i \in I}$  est une famille de sous-groupes de  $G$  indexée par  $I$  alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .
- 5) Soient  $G'$  un autre groupe et  $f$  un homomorphisme de  $G$  vers  $G'$ .
- Si  $H$  est un sous-groupe de  $G$  alors  $f(H)$  est un sous-groupe de  $G'$ .
  - Si  $K$  est un sous-groupe de  $G'$  alors  $f^{-1}(K)$  est un sous-groupe de  $G$ .
  - $\ker f$  est un sous-groupe de  $G$ .
- 6) Si  $G$  est multiplicatif alors :
- $\forall a \in G : \{a^k \mid k \in \mathbb{Z}\}$  est un sous-groupe de  $G$ .
  - Si  $H$  est un sous-groupe de  $G$  alors pour tout élément  $a$  de  $H$  :  

$$\{a^k \mid k \in \mathbb{Z}\} \subset H.$$
- 7) Si  $G$  est additif alors :
- $\forall a \in G : \{ka \mid k \in \mathbb{Z}\}$  est un sous-groupe de  $G$ .
  - Si  $H$  est un sous-groupe de  $G$  alors pour tout élément  $a$  de  $H$  :  

$$\{ka \mid k \in \mathbb{Z}\} \subset H.$$
- 8)  $\{1, -1\}$  est un sous-groupe des groupes multiplicatifs  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$  et  $\mathbb{C}^*$ .
- 7)  $\forall a \in \mathbb{Z} : a\mathbb{Z} = \mathbb{Z}a = \{ka \mid k \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .
- 8) Les sous-groupes de  $(\mathbb{Z}, +)$  sont les parties de  $\mathbb{Z}$  de la forme  $n\mathbb{Z}$  telle que  $n \in \mathbb{N}$ .

### Démonstration :

- 1) Soit  $\star$  la loi de  $G$ .
- Puisque  $(G, \star)$  est un groupe alors  $G$  est un sous-groupes de lui même.
  - $e \in \{e\} \Rightarrow \{e\} \neq \emptyset$ .  
 $\forall x, y \in \{e\} : x = y = e \Rightarrow x \star y = e \star e = e \in \{e\}$ .  
 Soient  $x$  un élément quelconque de  $\{e\}$  et  $x'$  son symétrique dans  $G$ .  
 $x \in \{e\} \Rightarrow x = e \Rightarrow x' = e \in \{e\}$ .  
 Donc  $\{e\}$  est un sous-groupe de  $G$ .
- 2) Soit  $\star$  la loi de  $G$ .
- Supposons que  $H$  et  $K$  sont des sous-groupes de  $G$ .
- Alors :  $[e \in H \text{ et } e \in K] \Rightarrow e \in H \cap K \Rightarrow H \cap K \neq \emptyset$ .
  - Soient  $x$  et  $y$  deux éléments quelconques de  $H \cap K$ , et soit  $y'$  le symétrique de  $y$  dans  $G$ .  

$$x, y \in H \cap K \Rightarrow [x, y \in H \text{ et } x, y \in K] \Rightarrow [x \star y' \in H \text{ et } x \star y' \in K] \\ \Rightarrow x \star y' \in H \cap K.$$
- Donc  $H \cap K$  est un sous-groupe de  $G$ .
- 3) Soient  $\star$  la loi de  $G$  et  $E$  un ensemble non vide de sous-groupes de  $G$ .
- Puisque  $e$  appartient à tous les éléments de  $E$  alors  $e$  appartient à  $\bigcap_{H \in E} H$ .  
 Donc :  $\bigcap_{H \in E} H \neq \emptyset$ .
  - Soient  $x$  et  $y$  deux éléments quelconques de  $\bigcap_{H \in E} H$ , et soit  $y'$  le symétrique de  $y$  dans  $G$ .  

$$x, y \in \bigcap_{H \in E} H \Rightarrow [\forall H \in E : x, y \in H] \Rightarrow [\forall H \in E : x \star y' \in H] \Rightarrow x \star y' \in \bigcap_{H \in E} H.$$
- Donc  $\bigcap_{H \in E} H$  est un sous-groupe de  $G$ .

4) Soient  $\star$  la loi de  $G$ ,  $I$  est un ensemble non vide et  $(H_i)_{i \in I}$  une famille de sous-groupes de  $G$  indexée par  $I$ .

- $e \in \bigcap_{i \in I} H_i$  (car on a :  $\forall i \in I : e \in H_i$ ). Donc :  $\bigcap_{i \in I} H_i \neq \emptyset$ .
- Soient  $x$  et  $y$  deux éléments quelconques de  $\bigcap_{i \in I} H_i$ , et soit  $y'$  le symétrique de  $y$  dans  $G$ .

$$x, y \in \bigcap_{i \in I} H_i \Rightarrow [\forall i \in I : x, y \in H_i] \Rightarrow [\forall i \in I : x \star y' \in H_i] \Rightarrow x \star y' \in \bigcap_{i \in I} H_i.$$

Donc  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .

5) Soient  $\star$  la loi de  $G$  et  $\star'$  la loi de  $G'$ .

a) Soit  $H$  un sous-groupe de  $G$ .

- $H \neq \emptyset \Rightarrow f(H) \neq \emptyset$ .
- Soient  $x$  et  $y$  deux éléments quelconques de  $f(H)$ , et soit  $y'$  le symétrique de  $y$  dans  $G'$ .

$$x, y \in f(H) \Rightarrow \exists a, b \in H \text{ tq : } x = f(a) \text{ et } y = f(b).$$

Soit  $b'$  le symétrique de  $b$  dans  $G$ .

Puisque  $H$  est un sous-groupe de  $G$  et puisque  $a, b \in H$  alors  $a \star b' \in H$ .

$$\text{Donc : } x \star' y' = f(a) \star' f(b)' = f(a) \star' f(b') = f(a \star b') \in f(H).$$

Ce qui montre que  $f(H)$  est un sous-groupe de  $G'$ .

b) Soient  $K$  est un sous-groupe de  $G'$  et  $e'$  l'élément neutre de  $G'$ .

- $f(e) = e' \in K \Rightarrow e \in f^{-1}(K) \Rightarrow f^{-1}(K) \neq \emptyset$ .
- Soient  $a$  et  $b$  deux éléments quelconques de  $f^{-1}(K)$ , et soit  $b'$  le symétrique de  $b$  dans  $G$ .

$$a, b \in f^{-1}(K) \Rightarrow f(a), f(b) \in K.$$

Puisque  $b'$  est le symétrique de  $b$  dans  $G$  alors  $f(b')$  est le symétrique de  $f(b)$  dans  $G'$ . Donc  $f(b') \in K$  (car  $K$  est un sous-groupe de  $G'$ ).

$$\text{Par suite : } f(a \star b') = f(a) \star' f(b') = f(a) \star' f(b)' \in K \Rightarrow a \star b' \in f^{-1}(K).$$

Ce qui montre que  $f^{-1}(K)$  est un sous-groupe de  $G$ .

c) Soit  $e'$  l'élément neutre de  $G'$ .

Puisque  $\{e'\}$  est un sous-groupe de  $G'$  alors  $\ker f = f^{-1}(\{e'\})$  est un sous-groupe de  $G$ .

6) Supposons que  $G$  est multiplicatif.

a) Soit  $a$  un éléments quelconques de  $G$ .

$$\text{Puisque l'application suivante : } f: \mathbb{Z} \rightarrow G \\ k \mapsto f(k) = a^k$$

est un homomorphisme de  $\mathbb{Z}$  vers  $G$  alors :

$$\{a^k \text{ tq : } k \in \mathbb{Z}\} = f(\mathbb{Z}) \text{ est un sous-groupe de } G.$$

b) Soient  $H$  un sous-groupe de  $G$  et  $a$  un élément quelconque de  $H$ .

Puisque  $H$  est un sous-groupe de  $(G, \cdot)$  alors  $(H, \cdot)$  est un groupe.

$$\text{Donc } \{a^k \text{ tq : } k \in \mathbb{Z}\} \subset H. (\text{car } a \text{ est un élément de } H).$$

7) Supposons que  $G$  est additif.

a) Soit  $a$  un éléments quelconques de  $G$ .

$$\text{Puisque l'application suivante : } f: \mathbb{Z} \rightarrow G \\ k \mapsto f(k) = ka$$

est un homomorphisme de  $\mathbb{Z}$  vers  $G$  alors :

$$\{ka \text{ tq : } k \in \mathbb{Z}\} = f(\mathbb{Z}) \text{ est un sous-groupe de } G.$$

b) Soient  $H$  un sous-groupe de  $G$  et  $a$  un élément quelconque de  $H$ .  
 Puisque  $H$  est un sous-groupe de  $(G, +)$  alors  $(H, +)$  est un groupe.  
 Donc  $\{ka \text{ tq } k \in \mathbb{Z}\} \subset H$ . (car  $a$  est un élément de  $H$ ).

8) •  $\{1, -1\} \neq \emptyset$  (car  $1 \in \{1, -1\}$ ).

•  $\forall x, y \in \{1, -1\}$  :

- Si  $x = 1$  :  $xy = 1y = y \in \{1, -1\}$ .

- Si  $y = 1$  :  $xy = x1 = x \in \{1, -1\}$ .

- Si  $x \neq 1$  et  $y \neq 1$  : alors :  $x = y = -1 \Rightarrow xy = (-1)(-1) = 1 \in \{1, -1\}$ .

•  $1^{-1} = 1 \in \{1, -1\}$  (car 1 est l'élément neutre).

$(-1)(-1) = 1 \Rightarrow (-1)^{-1} = -1 \in \{1, -1\}$ .

Donc  $\{1, -1\}$  est un sous-groupe des groupes multiplicatifs  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$  et  $\mathbb{C}^*$ .

### Notation 2-2-5 :

Pour tout entier relatif  $n$  on note par  $n\mathbb{Z}$ , l'ensemble  $n\mathbb{Z} = \{nk \text{ tq } k \in \mathbb{Z}\}$ .

C'est à dire :  $\forall n \in \mathbb{Z} : n\mathbb{Z} = \{nk \text{ tq } k \in \mathbb{Z}\}$ .

### Remarque 2-2-6 :

1) Pour tout entier relatif  $n$ ,  $n\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

$\forall n \in \mathbb{Z} : n\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

2) Si  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors pour tout élément  $n$  de  $H$ ,  $n\mathbb{Z}$  est contenu dans  $H$ .

C'est à dire si  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors :  $\forall n \in H : n\mathbb{Z} \subset H$ .

3) Si  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors pour tout élément  $n$  de  $H$ , la valeur absolue de  $n$  appartient à  $H$ .

C'est à dire si  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors :  $\forall n \in H : |n| \in H$ .

4) Pour tout entier relatif  $n$ ,  $n\mathbb{Z} = |n|\mathbb{Z}$ .

5) Si  $n$  et  $m$  sont des entiers relatifs alors :

i)  $n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m|n$ .

ii)  $n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow |n| = |m| \Leftrightarrow [n = m \text{ ou } n = -m]$ .

### Démonstration :

1) Soit  $n$  un entier relatif.

D'après la propriété 2-2-4-7) a),  $n\mathbb{Z} = \{nk \text{ tq } k \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

2) Soient  $H$  un sous-groupe de  $(\mathbb{Z}, +)$  et  $n$  élément quelconque  $n$  de  $H$ .

D'après la propriété 2-2-4-7) b),  $n\mathbb{Z} = \{nk \text{ tq } k \in \mathbb{Z}\} \subset H$ .

3) Soient  $H$  un sous-groupe de  $(\mathbb{Z}, +)$  et  $n$  élément quelconque  $n$  de  $H$ .

- Si  $n$  est positif : alors  $|n| = n \in H$ .

- Si  $n$  est négatif : alors  $|n| = -n \in H$ .

4) Soit  $n$  un entier relatif.

- Si  $n$  est positif : alors  $|n| = n$ . Donc :  $n\mathbb{Z} = |n|\mathbb{Z}$ .

- Si  $n$  est négatif : alors  $|n| = -n$ .

• Puisque  $n\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$  et puisque  $n \in n\mathbb{Z}$  alors  $|n| \in n\mathbb{Z}$ .

Donc :  $|n|\mathbb{Z} \subset n\mathbb{Z}$ .

• Puisque  $|n|\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$  et puisque  $n = -|n| \in |n|\mathbb{Z}$  alors  $n\mathbb{Z} \subset |n|\mathbb{Z}$ .

Ce qui montre que  $n\mathbb{Z} = |n|\mathbb{Z}$ .

5) Soient  $n$  et  $m$  deux entiers relatifs.

i)  $\Rightarrow$  ) Si  $n\mathbb{Z} \subset m\mathbb{Z}$  :

$$n = n1 \in n\mathbb{Z} \subset m\mathbb{Z} \Rightarrow [\exists k \in \mathbb{Z} \text{ tq : } n = mk] \Rightarrow m|n.$$

$\Leftarrow$  ) Si  $m|n$  :

$$\text{Alors : } \exists k \in \mathbb{Z} \text{ tq : } n = mk.$$

$$\forall a \in n\mathbb{Z} : \exists u \in \mathbb{Z} \text{ tq : } a = nu. \text{ Donc : } a = (mk)u = m(ku) \in m\mathbb{Z}.$$

$$\text{Par suite } n\mathbb{Z} \subset m\mathbb{Z}.$$

Ce qui prouve que  $n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m|n$ .

$$\begin{aligned} \text{ii) } n\mathbb{Z} = m\mathbb{Z} &\Leftrightarrow [n|\mathbb{Z} = |m|\mathbb{Z}] \Leftrightarrow [n|\mathbb{Z} \subset |m|\mathbb{Z} \text{ et } |m|\mathbb{Z} \subset n|\mathbb{Z}] \Leftrightarrow [|m|||n| \text{ et } |n|||m|] \\ &\Leftrightarrow |n| = |m| \Leftrightarrow [n = m \quad \text{ou} \quad n = -m]. \end{aligned}$$

### **Théorème 2-2-7 :**

Les sous-groupes de  $(\mathbb{Z}, +)$  sont les parties de  $\mathbb{Z}$  de la forme  $n\mathbb{Z}$  telles que  $n \in \mathbb{N}$ .

### **Démonstration :**

- Les parties de  $\mathbb{Z}$  de la forme  $n\mathbb{Z}$  telles que  $n \in \mathbb{N}$  sont tous des sous-groupes de  $(\mathbb{Z}, +)$ .

- Soit  $H$  un sous-groupe quelconque de  $(\mathbb{Z}, +)$ .

- Si  $H = \{0\}$  :

$$\text{Alors : } H = \{0\} = 0\mathbb{Z} \text{ et } 0 \in \mathbb{N}.$$

- Si  $H \neq \{0\}$  :

Soit  $u$  élément non nul de  $H$ .  $u \neq 0 \Rightarrow |u| > 0 \Rightarrow |u| \in \mathbb{N}^*$ . Alors :  $|u| \in H \cap \mathbb{N}^*$ .

Par suite  $H \cap \mathbb{N}^*$  est une partie non vide de  $\mathbb{N}^*$ .

Soit  $n$  le plus petit élément de  $H \cap \mathbb{N}^*$ .

$$\star n \in H \cap \mathbb{N}^* \subset H \Rightarrow n\mathbb{Z} \subset H.$$

$$\star \text{ Soit } a \text{ élément quelconque de } H. \text{ Il existe } q, r \in \mathbb{Z} \text{ tels que : } \begin{cases} a = nq + r \\ 0 \leq r < n \end{cases}.$$

$$n \in H \Rightarrow nq \in n\mathbb{Z} \subset H. \text{ Alors : } r = a - nq \in H.$$

$$\text{Supposons que } r \text{ est non nul. Alors : } r \in H \cap \mathbb{N}^* \subset H \Rightarrow r \geq n.$$

$$\text{Ce qui est absurde. Donc } r \text{ est nul. Par suite } a = nq + r = nq + 0 = nq \in n\mathbb{Z}.$$

$$\text{Ce qui montre que } H = n\mathbb{Z}.$$

## **2-3 - Classes modulo un sous-groupe :**

### **Définition et notations 2-3-1 :**

Soient  $(G, *)$  un groupe et  $H$  un sous-groupe de  $G$ .

\* Pour tout élément  $a$  de  $G$ ,  $a * H = \{a * h \text{ tq : } h \in H\}$  est appelé la classe à gauche de  $a$  modulo  $H$  ou la classe à gauche de  $a$ .

\* Pour tout élément  $a$  de  $G$ ,  $H * a = \{h * a \text{ tq : } h \in H\}$  est appelé la classe à droite de  $a$  modulo  $H$  la classe à droite de  $a$ .

\* Si  $G$  est abélien alors pour tout élément  $a$  de  $G$ ,  $a * H = H * a$  est appelé la classe de  $a$  modulo  $H$  ou la classe de  $a$  et noté aussi.:  $\overline{(a)}_H$  ou  $\bar{a}$ .

\*  $G \not\sim H = \{a * H \text{ tq : } a \in G\} \subset \mathcal{P}(G)$  est l'ensemble des classes à gauche des éléments de  $G$  modulo  $H$ .

- \*  $G \nearrow H = \{H * a \text{ tq : } a \in G\} \subset \mathcal{P}(G)$  est l'ensemble des classes à droite des éléments de  $G$  modulo  $H$ .
- \* Si  $G \nearrow H$  est fini, on dit que  $H$  est d'indice fini dans  $G$ .
- \* Si  $H$  est d'indice fini dans  $G$ , le cardinal de  $G \nearrow H$  est appelé l'indice de  $H$  dans  $G$  et noté  $[G : H]$ .  
C'est à si  $H$  est d'indice fini dans  $G$ ,  $[G : H] = |G \nearrow H|$ .
- \* Si  $G \nearrow H$  est infini, on dit que  $H$  est d'indice infini dans  $G$ .
- \* Si  $G$  est abélien :  $G/H = G \nearrow H = G \nearrow H = \{(\overline{a})_H \text{ tq : } a \in G\} = \{\bar{a} \text{ tq : } a \in G\}$  est l'ensemble des classes de  $a$  modulo  $H$  ou l'ensemble des classes de  $a$ .
- \* Si  $G$  est abélien, l'application suivante :  $p : G \rightarrow G/H$   
$$a \mapsto p(a) = \overline{(a)}_H$$
qui est surjective est appelée la surjection canonique de  $G$  vers  $G/H$ .

### Exemples 2-3-2 :

Soit  $n$  un entier natrel.

Pour tout entier relatif  $k$ ,  $k + n\mathbb{Z}$  est appelé la classe de  $k$  modulo  $n$  ou la classe de  $k$ , et noté  $\bar{k}$  (modulo  $n$ ) ou  $\bar{k}$ .

Soient  $a$  et  $b$  deux entier relatifs. Si  $a + n\mathbb{Z} = b + n\mathbb{Z}$  on dit que  $a$  congru à  $b$  modulo  $n$  et on note :  $a \equiv b$  (modulo  $n$ ) ou  $a \equiv b$ .

- 1)  $\mathbb{Z} \nearrow n\mathbb{Z} = \mathbb{Z} \nearrow n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ .
- 2)  $\forall a, b \in \mathbb{Z} : a \equiv b \text{ (modulo } n) \Leftrightarrow a - b \in n\mathbb{Z}$ .
- 3) Si  $n = 0$ .
  - a)  $\forall k \in \mathbb{Z} : \bar{k} \text{ (modulo } 0) = \{k\}$ .
  - b)  $\mathbb{Z}/\{0\} = \mathbb{Z}/0\mathbb{Z} = \{\{k\} \text{ tq : } k \in \mathbb{Z}\}$ .
  - c)  $0\mathbb{Z} = \{0\}$  est d'indice infini dans  $\mathbb{Z}$ .
- 4) Si  $n = 1$ .
  - a)  $\forall k \in \mathbb{Z} : \bar{k} \text{ (modulo } 1) = \mathbb{Z}$ .
  - b)  $\mathbb{Z}/\mathbb{Z} = \mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\}$ .
  - c)  $1\mathbb{Z} = \mathbb{Z}$  est d'indice fini dans  $\mathbb{Z}$  et on a  $[\mathbb{Z} : \mathbb{Z}] = [\mathbb{Z} : 1\mathbb{Z}] = 1$ .
- 5) Si  $n \neq 0$ .
  - a)  $\bar{0}, \dots, \overline{n-1}$  sont distincts deux à deux.
  - b)  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$ .
  - c)  $n\mathbb{Z}$  est d'indice fini dans  $\mathbb{Z}$  et on a  $[\mathbb{Z} : n\mathbb{Z}] = n$ .

### Démonstration :

- 1) Puisque  $\mathbb{Z}$  est un groupe abélien alors :  $\mathbb{Z} \nearrow n\mathbb{Z} = \mathbb{Z} \nearrow n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ .
- 2)  $\forall a, b \in \mathbb{Z} : a \equiv b \text{ (modulo } n) \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \Leftrightarrow -b + (a + n\mathbb{Z}) = -b + (b + n\mathbb{Z})$   

$$\Leftrightarrow (-b + a) + n\mathbb{Z} = (-b + b) + n\mathbb{Z} = 0 + n\mathbb{Z} = n\mathbb{Z}$$

$$\Leftrightarrow (a - b) + n\mathbb{Z} = n\mathbb{Z}$$

$$\Leftrightarrow a - b \in n\mathbb{Z}.$$
- 3) Supposons que  $n = 0$ .
  - a)  $\forall k \in \mathbb{Z} : \bar{k} \text{ (modulo } 0) = k + 0\mathbb{Z} = k + \{0\} = \{k\}$ .
  - b)  $\mathbb{Z}/\{0\} = \mathbb{Z}/0\mathbb{Z} = \{\bar{k} \text{ (modulo } 0) \text{ tq : } k \in \mathbb{Z}\} = \{\{k\} \text{ tq : } k \in \mathbb{Z}\}$ .
  - c) Puisque  $\mathbb{Z}/\{0\} = \{\{k\} \text{ tq : } k \in \mathbb{Z}\}$  est un ensemble infini alors  $0\mathbb{Z} = \{0\}$  est d'indice infini dans  $\mathbb{Z}$ .

4) Supposons que  $n = 1$ .

a)  $\forall k \in \mathbb{Z} : \bar{k} \text{ (modulo } 1) = k + 1\mathbb{Z} = k + \mathbb{Z} = \mathbb{Z}$ .

b)  $\mathbb{Z}/\mathbb{Z} = \mathbb{Z}/1\mathbb{Z} = \{\bar{k} \text{ (modulo } 0) \text{ tq : } k \in \mathbb{Z}\} = \{\mathbb{Z}\}$ .

c) Puisque  $\mathbb{Z}/\mathbb{Z} = \mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\}$  alors  $\mathbb{Z} = 1\mathbb{Z}$  est d'indice fini dans  $\mathbb{Z}$  et on a  $[\mathbb{Z} : \mathbb{Z}] = [\mathbb{Z} : 1\mathbb{Z}] = 1$ .

5) Supposons que  $n \neq 0$  et posons  $I = \{0, \dots, n-1\}$ .

a) Soient  $i$  et  $j$  deux éléments quelconques de  $I$  tels que :  $\begin{cases} i \geq j \\ \bar{i} = \bar{j} \end{cases}$ .

$i \geq j \Rightarrow i - j \geq 0$ .  $i - j \leq i \leq n-1$  (car  $j \geq 0$  et  $i \in I$ ). Donc  $i - j \in I$ .

$\bar{i} = \bar{j} \Rightarrow i \equiv j \text{ (modulo } n) \Rightarrow i - j \in n\mathbb{Z} \Rightarrow \exists k \in \mathbb{Z} \text{ tq : } i - j = kn$ .

Alors :  $kn = i - j \in I \Rightarrow 0 \leq kn \leq n-1 < n \Rightarrow 0 \leq k < 1 \Rightarrow k = 0 \Rightarrow i - j = 0 \Rightarrow i = j$ .

Donc  $\bar{0}, \dots, \overline{n-1}$  sont distincts deux à deux.

b) Soit  $x$  un élément quelconque de  $\mathbb{Z}/n\mathbb{Z}$ .

Il existe un entier relatif  $k$  tel que  $x = \bar{k}$ .  $k \in \mathbb{Z} \Rightarrow \exists q, i \in \mathbb{Z} \text{ tq : } \begin{cases} k = qn + i \\ 0 \leq i < n \end{cases}$ .

$0 \leq i < n \Rightarrow i \in I$ .

$k = qn + i \Rightarrow k - i = qn \in n\mathbb{Z} \Rightarrow k \equiv i \text{ (modulo } n) \Rightarrow x = \bar{k} = \bar{i} \in \{\bar{0}, \dots, \overline{n-1}\}$ .

Donc  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$ .

c) D'après b)  $n\mathbb{Z}$  est d'indice fini dans  $\mathbb{Z}$  et on a :

$$[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = |\{\bar{0}, \dots, \overline{n-1}\}| = n.$$

### Propriétés 2-3-3 :

Soient  $(G, *)$  un groupe,  $e$  son élément neutre et  $H$  un sous-groupe de  $G$ .

1)  $H \in (G \setminus H)$  et  $H \in (G \nearrow H)$ .

2)  $\forall a \in H : a * H = H * a = H$ .

3)  $\forall a \in G : a * H = H \Leftrightarrow a \in H$ .

4)  $\forall a \in G : H * a = H \Leftrightarrow a \in H$ .

5)  $H = G \Leftrightarrow G \in (G \setminus H) \Leftrightarrow G \in (G \nearrow H)$ .

6)  $G \setminus G = G \nearrow G = \{G\}$ .

7) Si  $H = \{e\}$ .

a)  $\forall a \in G : a * \{e\} = \{e\} * a = \{a\}$ .

b)  $G \setminus \{e\} = G \nearrow \{e\} = \{\{a\} \text{ tq : } a \in G\}$ .

c)  $G \setminus \{e\}$  et  $G \nearrow \{e\}$  sont équipotents à  $G$ .

d)  $\{e\}$  est d'indice fini dans  $G$  si et seulement si  $G$  est d'ordre fini, et dans ce cas :  $[G : \{e\}] = |G|$ .

8) La relation  $R$  définie dans  $G$  par :

$\forall a, b \in G : aRb \Leftrightarrow a' * b \in H$  (où  $a'$  est le symétrique de  $a$ ).

est une relation d'équivalence

9)  $G \setminus H$  est la partition de  $G$  associée à la relation d'équivalence  $R$  suivante :

$\forall a, b \in G : aRb \Leftrightarrow a' * b \in H$  (où  $a'$  est le symétrique de  $a$ ).

10)  $\forall A \in G \setminus H$  et  $\forall a \in G : A = a * H \Leftrightarrow a \in A$ .

11) La relation  $S$  définie dans  $G$  par :

$\forall a, b \in G : aSb \Leftrightarrow b * a' \in H$  (où  $a'$  est le symétrique de  $a$ ).

est une relation d'équivalence.



- 12)  $G \nearrow H$  est la partition de  $G$  associée à la relation d'équivalence  $S$  suivante :  
 $\forall a, b \in G : aSb \Leftrightarrow b * a' \in H$  (où  $a'$  est le symétrique de  $a$ ).
- 13)  $\forall A \in G \nearrow H$  et  $\forall a \in G : A = H * a \Leftrightarrow a \in A$ .
- 14) Les éléments de  $G \swarrow H$  et les éléments de  $G \nearrow H$  sont tous équipotents à  $H$ .
- 15) Si  $H$  est d'ordre fini alors :  
 a) tous les éléments de  $G \swarrow H$  sont finis et on a :  $\forall A \in G \swarrow H : |A| = |H|$ .  
 b) tous les éléments de  $G \nearrow H$  sont finis et on a :  $\forall A \in G \nearrow H : |A| = |H|$ .
- 16)  $\forall a \in G : (a * H)' = H * a'$ .  
 Où  $(a * H)'$  est l'ensemble des symétriques éléments de  $a * H$  et  $a'$  est le symétrique de  $a$ .
- 17)  $\forall a \in G : (H * a)' = a' * H$ .  
 Où  $(H * a)'$  est l'ensemble des symétriques éléments de  $H * a$  et  $a'$  est le symétrique de  $a$ .
- 18) Les deux ensembles  $G \swarrow H$  et  $G \nearrow H$  sont équipotents.
- 19)  $H$  est d'indice fini dans  $G$  si et seulement si  $G \nearrow H$  est fini, et dans ce cas  
 $[G : H] = |G \nearrow H|$ .

### Démonstration :

- 1)  $H = e * H \in (G \swarrow H)$  et  $H = H * e \in (G \nearrow H)$ .
- 2)  $\forall a \in H$  :  
 $\subset$ )  $\forall x \in (a * H) : \exists h \in H$  tq :  $x = a * h \in H$ . Donc :  $a * H \subset H$ .  
 $\subset$ )  $\forall x \in (H * a) : \exists h \in H$  tq :  $x = h * a \in H$ . Donc :  $H * a \subset H$ .  
 $\supset$ ) Soit  $a'$  le symétrique de  $a$ .  

$$\forall x \in H : \begin{cases} x = e * x = (a * a') * x = a * (a' * x) \in (a * H) \\ x = x * e = x * (a' * a) = (x * a') * a \in (H * a) \end{cases}$$
 Alors :  $H \subset a * H$  et  $H \subset H * a$ .  
 Ce qui montre que :  $a * H = H * a = H$ .
- 3)  $\forall a \in G$  :  
 $\Rightarrow$ ) Si  $a * H = H$  : Alors :  $a = a * e \in a * H = H$ . Donc  $a \in H$ .  
 $\Leftarrow$ ) Si  $a \in H$  : Alors (d'après 2)),  $a * H = H$ .  
 Ce qui montre que :  $a * H = H \Leftrightarrow a \in H$ .
- 4)  $\forall a \in G$  :  
 $\Rightarrow$ ) Si  $H * a = H$  : Alors :  $a = e * a \in H * a = H$ . Donc  $a \in H$ .  
 $\Leftarrow$ ) Si  $a \in H$  : Alors (d'après 2)),  $H * a = H$ .  
 Ce qui montre que :  $H * a = H \Leftrightarrow a \in H$ .
- 5) •  $H = G \Rightarrow G = H \in (G \swarrow H)$  et  $G = H \in (G \nearrow H)$ .  
 • Si  $G \in (G \swarrow H)$  :  
 Alors il existe un élément  $a$  de  $G$  tel que  $G = a * H$ .  
 Donc :  $H = e * H = (a' * a) * H = a' * (a * H) = a' * G = G$   
 où  $a'$  est le symétrique de  $a$ .  
 • Si  $G \in (G \nearrow H)$  :  
 Alors il existe un élément  $a$  de  $G$  tel que  $G = H * a$ .  
 Donc :  $H = H * e = H * (a * a') = (H * a) * a' = G * a' = G$ .  
 où  $a'$  est le symétrique de  $a$ .  
 Par suite on a :  $G \in (G \swarrow H) \Rightarrow H = G$  et  $G \in (G \nearrow H) \Rightarrow H = G$ .  
 Ce qui prouve que :  $H = G \Leftrightarrow G \in (G \swarrow H) \Leftrightarrow G \in (G \nearrow H)$ .

$$6) \bullet [G \in G \swarrow G \text{ et } G \in G \nearrow G] \Rightarrow [\{G\} \subset G \swarrow G \text{ et } \{G\} \subset G \nearrow G].$$

$$\bullet \forall A \in G \swarrow G : \exists a \in G \text{ tq : } A = a * G = G \in \{G\}.$$

$$\text{Alors : } G \swarrow G \subset \{G\}.$$

$$\bullet \forall A \in G \nearrow G : \exists a \in G \text{ tq : } A = G * a = G \in \{G\}.$$

$$\text{Alors : } G \nearrow G \subset \{G\}.$$

$$\text{Ce qui montre que : } G \swarrow G = G \nearrow G = \{G\}.$$

$$7) \text{ Supposons } H = \{e\}.$$

$$a) \forall a \in G :$$

$$\forall x \in G : x \in a * \{e\} \Leftrightarrow x = a * e = a \in \{a\}. \text{ Donc : } a * \{e\} = \{a\}.$$

$$\forall x \in G : x \in \{e\} * a \Leftrightarrow x = e * a = a \in \{a\}. \text{ Donc : } \{e\} * a = \{a\}.$$

$$\text{Ce qui prouve que : } a * \{e\} = \{e\} * a = \{a\}.$$

$$b) G \swarrow \{e\} = \{a * \{e\} \text{ tq : } a \in G\} = \{\{a\} \text{ tq : } a \in G\}.$$

$$G \nearrow \{e\} = \{\{e\} * a \text{ tq : } a \in G\} = \{\{a\} \text{ tq : } a \in G\}.$$

$$\text{Donc : } G \swarrow \{e\} = G \nearrow \{e\} = \{\{a\} \text{ tq : } a \in G\}.$$

$$c) \text{ Puisque (d'après b)), } G \swarrow \{e\} = G \nearrow \{e\} = \{\{a\} \text{ tq : } a \in G\} \text{ alors :}$$

$$G \swarrow \{e\} \text{ et } G \nearrow \{e\} \text{ sont équipotents à } G.$$

$$d) [\{e\} \text{ est d'indice fini dans } G] \Leftrightarrow [G \swarrow \{e\} \text{ est fini}]$$

$$\Leftrightarrow [G \text{ est d'ordre fini}] \text{ (car } G \swarrow \{e\} \text{ est équipotent à } G).$$

$$\text{Dans ce cas : } [G : \{e\}] = |G| \text{ (car } G \swarrow \{e\} \text{ est équipotent à } G).$$

$$8) \bullet \forall a \in G : a' * a = e \in H \Rightarrow aRa. \text{ Donc } R \text{ est réflexive.}$$

$$\bullet \forall a, b \in G : aRb \Rightarrow a' * b \in H \text{ (où } a' \text{ est le symétrique de } a)$$

$$\Rightarrow (a' * b)' \in H \text{ (où } (a' * b)' \text{ est le symétrique de } a' * b)$$

$$\Rightarrow b' * b \in H \text{ (où } b' \text{ est le symétrique de } b)$$

$$\Rightarrow bRa.$$

$$\text{Donc } R \text{ est symétrique.}$$

$$\bullet \forall a, b, c \in G :$$

$$\begin{cases} aRb \\ bRc \end{cases} \Rightarrow \begin{cases} a' * b \in H \text{ (où } a' \text{ est le symétrique de } a) \\ b' * c \in H \text{ (où } b' \text{ est le symétrique de } b) \end{cases}$$

$$\Rightarrow (a' * b) * (b' * c) \in H \Rightarrow a' * (b * b') * c \in H \Rightarrow a' * e * c \in H$$

$$\Rightarrow a' * c \in H.$$

$$\text{Donc } R \text{ est transitive.}$$

$$\text{Ce qui montre que } R \text{ est une relation d'équivalence dans } G$$

$$9) \forall A \in G \swarrow H : \exists a \in G \text{ tq : } A = a * H$$

$$\forall x \in G :$$

$$x \in A = a * H \Leftrightarrow [\exists h \in H \text{ tq : } x = a * h]$$

$$\Leftrightarrow [\exists h \in H \text{ tq : } a' * x = a' * (a * h) = (a' * a) * h = e * h = h]$$

$$\Leftrightarrow a' * x \in H \Leftrightarrow aRx \Leftrightarrow xRa$$

$$\Leftrightarrow x \in \overline{(a)}_R.$$

$$\text{Alors : } A = \overline{(a)}_R.$$

$$\text{Ce qui montre que } G \swarrow H \text{ est la partition de } G \text{ associée à la relation d'équivalence } R \text{ suivante : } \forall a, b \in G : aRb \Leftrightarrow a' * b \in H \text{ (où } a' \text{ est le symétrique de } a).$$

$$10) \forall A \in G \swarrow H \text{ et } \forall a \in G :$$

$$A \in G \swarrow H \Rightarrow A \in G/R.$$

$$\text{Donc : } A = a * H \Leftrightarrow A = \overline{(a)}_R \Leftrightarrow a \in A.$$

- 11) •  $\forall a \in G : a \star a' = e \in H \Rightarrow aSa$ . Donc  $S$  est réflexive.  
 •  $\forall a, b \in G : aSb \Rightarrow b \star a' \in H$  (où  $a'$  est le symétrique de  $a$ )  
 $\Rightarrow (b \star a')' \in H$  (où  $(b \star a')'$  est le symétrique de  $b \star a'$ )  
 $\Rightarrow a \star b' \in H$  (où  $b'$  est le symétrique de  $b$ )  
 $\Rightarrow bSa$ .

Donc  $S$  est symétrique.

- $\forall a, b, c \in G :$   

$$\begin{cases} aSb \\ bSc \end{cases} \Rightarrow \begin{cases} b \star a' \in H \text{ (où } a' \text{ est le symétrique de } a) \\ c \star b' \in H \text{ (où } b' \text{ est le symétrique de } b) \end{cases}$$
  
 $\Rightarrow (c \star b') \star (b \star a') \in H \Rightarrow c \star (b' \star b) \star a' \in H \Rightarrow c \star e \star a' \in H$   
 $\Rightarrow c \star a' \in H$ .

Donc  $S$  est transitive.

Ce qui montre que  $S$  est une relation d'équivalence dans  $G$

- 12)  $\forall A \in G \nearrow H : \exists a \in G \text{ tq } A = H \star a$

$\forall x \in G :$

$$\begin{aligned} x \in A = H \star a &\Leftrightarrow [\exists h \in H \text{ tq } : x = h \star a] \\ &\Leftrightarrow [\exists h \in H \text{ tq } : x \star a' = (h \star a) \star a' = h \star (a \star a') = h \star e = h] \\ &\Leftrightarrow x \star a' \in H \Leftrightarrow aSx \Leftrightarrow xSa \\ &\Leftrightarrow x \in \overline{(a)}_S. \end{aligned}$$

Alors :  $A = \overline{(a)}_S$ .

Ce qui montre que  $G \nearrow H$  est la partition de  $G$  associée à la relation d'équivalence  $S$  suivante :  $\forall a, b \in G : aSb \Leftrightarrow b \star a' \in H$  (où  $a'$  est le symétrique de  $a$ ).

- 13)  $\forall A \in G \nearrow H$  et  $\forall a \in G :$

$A \in G \nearrow H \Rightarrow A \in G/S$ .

Donc :  $A = H \star a \Leftrightarrow A = \overline{(a)}_S \Leftrightarrow a \in A$ .

- 14) • Soient  $A$  un élément quelconque de  $G \nearrow H$  et  $a$  un élément de  $A$ .

Montrons que l'application suivante :  $f : H \rightarrow A = a \star H$   
 $h \mapsto f(h) = a \star h$

est une bijection de  $H$  vers  $A$ .

- $\forall h, k \in H : f(h) = f(k) \Rightarrow a \star h = a \star k \Rightarrow h = k$ . Donc  $f$  est injective.
- $\forall x \in A : x \in A = a \star H \Rightarrow a \star H = A = x \star H$ .

Alors  $a' \star x \in H$  (où  $a'$  est le symétrique de  $a$ ) et on a :

$$f(a' \star x) = a \star (a' \star x) = (a \star a') \star x = e \star x = x.$$

Donc  $f$  est surjective.

Par suite  $f$  est une bijection de  $H$  vers  $A$ .

Ce qui montre que  $A$  est équipotent à  $H$ .

- Soient  $A$  un élément quelconque de  $G \nearrow H$  et  $a$  un élément de  $A$ .

Montrons que l'application suivante :  $g : H \rightarrow A = H \star a$   
 $h \mapsto g(h) = h \star a$

est une bijection de  $H$  vers  $A$ .

- $\forall h, k \in H : g(h) = g(k) \Rightarrow h \star a = k \star a \Rightarrow h = k$ . Donc  $f$  est injective.
- $\forall x \in A : x \in A = H \star a \Rightarrow H \star a = A = H \star x$ .

Alors  $x \star a' \in H$  (où  $a'$  est le symétrique de  $a$ ) et on a :

$$g(x \star a') = (x \star a') \star a = x \star (a' \star a) = x \star e = x.$$

Donc  $g$  est surjective.

Par suite  $f$  est une bijection de  $H$  vers  $A$ .

Ce qui montre que  $A$  est équipotent à  $H$ .

15) Supposons que  $H$  est d'ordre fini.

a) Soit  $A$  un élément quelconque de  $G \searrow H$

Puisque  $H$  est d'ordre fini et puisque  $A$  est équipotent à  $H$  alors  $A$  est aussi fini et on a  $|A| = |H|$ .

b) Soit  $A$  un élément quelconque de  $G \nearrow H$

Puisque  $H$  est d'ordre fini et puisque  $A$  est équipotent à  $H$  alors  $A$  est aussi fini et on a  $|A| = |H|$ .

16)  $\forall a \in G :$

$$\begin{aligned} \forall x \in G : x \in (a * H)' &\Leftrightarrow x' \in a * H \text{ (où } x' \text{ est le symétrique de } x) \\ &\Leftrightarrow x' * H = a * H \Leftrightarrow x * (x' * H) = x * (a * H) \\ &\Leftrightarrow (x * a) * H = (x * x') * H = e * H = H \Leftrightarrow x * a \in H \\ &\Leftrightarrow x \in H * a'. \end{aligned}$$

Donc :  $(a * H)' = H * a'$ , où  $(a * H)'$  est l'ensemble des symétriques des éléments de  $a * H$  et  $a'$  est le symétrique de  $a$ .

17)  $\forall a \in G :$

$$\begin{aligned} \forall x \in G : x \in (H * a)' &\Leftrightarrow x' \in H * a \text{ (où } x' \text{ est le symétrique de } x) \\ &\Leftrightarrow H * x' = H * a \Leftrightarrow (H * x') * x = (H * a) * x \\ &\Leftrightarrow H * (a * x) = H * (x' * x) = H * e = H \Leftrightarrow a * x \in H \\ &\Leftrightarrow x \in a' * H. \end{aligned}$$

Donc :  $(H * a)' = a' * H$ .

Où  $(H * a)'$  est l'ensemble des symétriques éléments de  $a * H$  et  $a'$  est le symétrique de  $a$ .

18) Soient  $f$  et  $g$  les deux applications suivantes :

$$f : G \searrow H \rightarrow G \nearrow H$$

$$A \mapsto f(A) = A' \text{ (où } A' \text{ est l'ensemble des symétriques des éléments de } A).$$

$$g : G \nearrow H \rightarrow G \searrow H$$

$$A \mapsto g(A) = A' \text{ (où } A' \text{ est l'ensemble des symétriques des éléments de } A).$$

$$\forall A \in G \searrow H : (g \circ f)(A) = g(f(A)) = g(A') = (A')' = A = id_{G \searrow H}(A).$$

$$\forall A \in G \nearrow H : (f \circ g)(A) = f(g(A)) = f(A') = (A')' = A = id_{G \nearrow H}(A).$$

$$\text{Alors : } \begin{cases} g \circ f = id_{G \searrow H} \\ f \circ g = id_{G \nearrow H} \end{cases} . \text{ Donc } f \text{ est une bijection de } G \searrow H \text{ vers } G \nearrow H.$$

Ce qui prouve que les deux ensembles  $G \searrow H$  et  $G \nearrow H$  sont équipotents.

19)  $[H \text{ est d'indice fini dans } G] \Leftrightarrow G \searrow H \text{ est fini} \Leftrightarrow G \nearrow H \text{ est fini}.$

$$\text{Dans ce cas : } [G : H] = |G \searrow H| = |G \nearrow H|.$$

### **Théorème 2-3-4 :**

Soient  $G$  un groupe et  $H$  un sous-groupe de  $G$ .

Pour que  $G$  soit d'ordre fini il faut et il suffit que  $H$  est d'ordre fini et  $H$  est d'indice fini dans  $G$ .

Dans ce cas on a la formule suivante appelé la formule de Lagrange :  $|G| = [G : H]|H|$ .

### **Démonstration :**

Puisque  $G \searrow H$  est une partition de  $G$  alors  $G$  est d'ordre fini si et seulement si  $G \searrow H$  est fini et tous les éléments de  $G \searrow H$  sont finis.

Donc  $G$  est d'ordre fini si et seulement si  $H$  est d'ordre fini et  $H$  est d'indice fini dans  $G$ .

$$\text{Dans ce cas on a alors : } |G| = \sum_{A \in G \searrow H} |A| = \sum_{A \in G \searrow H} |H| = [G : H]|H|.$$

**Corollaire 2-3-5 :**

Soient  $G$  un groupe et  $H$  un sous-groupe de  $G$ .

Si  $G$  est d'ordre fini alors l'ordre de  $H$  et l'indice de  $H$  dans  $G$  sont des diviseurs de l'ordre de  $G$ .

C'est à dire si  $G$  est d'ordre fini alors  $|H|$  et  $[G : H]$  sont des diviseurs de  $|G|$ .

**En effet :**

Supposons que  $G$  est d'ordre fini.

Puisqu'on a  $|G| = [G : H]|H|$  alors  $|H|$  et  $[G : H]$  sont des diviseurs de  $|G|$ .

**Corollaire 2-3-6 :**

Soient  $G$  un groupe et  $e$  son élément neutre.

Si  $G$  est fini d'ordre premier alors les seuls sous-groupes de  $G$  sont  $G$  et  $\{e\}$

**En effet :**

Supposons que  $G$  est fini d'ordre premier.

Puisque  $|H|$  est un diviseurs de  $|G|$  et puisque  $|G|$  est un nombre premier alors

$|H| = |G|$  ou  $|H| = 1$ . Donc  $H = G$  ou  $H = \{e\}$ .

Ce qui prouve que les seuls sous-groupes de  $G$  sont  $G$  et  $\{e\}$

**Corollaire 2-3-7 :**

Soit  $G$  un groupe fini d'ordre premier.

1) Si  $G$  est multiplicatif alors :

a)  $\forall a \in G - \{e\} : G = \{a^k \text{ tq } k \in \mathbb{Z}\}$  ( $e$  étant l'élément neutre de  $G$ ).

b)  $G$  est abélien.

2) Si  $G$  est additif alors :

a)  $\forall a \in G - \{0_G\} : G = \{ka \text{ tq } k \in \mathbb{Z}\}$ .

b)  $G$  est abélien.

**Démonstration :**

1) a) Soient  $a$  un élément quelconque de  $G$  distinct de l'élément neutre  $e$  de  $G$  et  $H = \{a^k \text{ tq } k \in \mathbb{Z}\}$ .

$H$  est un sous-groupe de  $G$  contenant  $a$ . Donc  $H \neq \{e\}$ .

Puisque (d'après le corollaire 2-3-6) les seuls sous-groupes de  $G$  sont  $G$  et  $\{e\}$ , et puisque  $H$  est sous-groupe de  $G$  distinct de  $\{e\}$  alors :

$G = H = \{a^k \text{ tq } k \in \mathbb{Z}\}$ .

b) Soient  $a$  un élément de  $G$  distinct de l'élément neutre  $e$  de  $G$ .

D'après a),  $G = H = \{a^k \text{ tq } k \in \mathbb{Z}\}$ .

$\forall x, y \in G : \exists n, m \in \mathbb{Z} \text{ tq } x = a^n \text{ et } y = a^m. xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx.$

Donc  $G$  est abélien.

2) a) Soient  $a$  un élément quelconque de  $G$  distinct de  $0_G$  et  $H = \{ka \text{ tq } k \in \mathbb{Z}\}$ .

$H$  est un sous-groupe de  $G$  contenant  $a$ . Donc  $H \neq \{0_G\}$ .

Puisque (d'après le corollaire 2-3-6) les seuls sous-groupes de  $G$  sont  $G$  et  $\{0_G\}$ , et puisque  $H$  est sous-groupe de  $G$  distinct de  $\{0_G\}$  alors :

$G = H = \{ka \text{ tq } k \in \mathbb{Z}\}$ .

b) Soient  $a$  un élément de  $G$  distinct de  $0_G$ .

D'après a),  $G = H = \{ka \text{ tq } k \in \mathbb{Z}\}$ .

$\forall x, y \in G : \exists n, m \in \mathbb{Z} \text{ tq } x = na \text{ et } y = ma$ .

$$x + y = na + ma = (n + m)a = (m + n)a = ma + na = y + x.$$

Donc  $G$  est abélien.

### Lemme 2-3-8 :

Soient  $(G, \star)$  un groupe abélien et  $H$  un sous-groupe de  $G$ .

Si  $a$  et  $b$  sont des éléments de  $G$  alors :  $\overline{(a)}_H \star \overline{(b)}_H = \overline{(a \star b)}_H$ . (c'est à dire  $(a \star)$ )

C'est à dire :  $\forall a, b \in G : (a \star H) \star (b \star H) = (a \star b) \star H$ .

### En effet :

$$\begin{aligned} \forall a, b \in G : \overline{(a)}_H \star \overline{(b)}_H &= (a \star H) \star (b \star H) = a \star (H \star b) \star H = a \star (b \star H) \star H \\ &= (a \star b) \star (H \star H) = (a \star b) \star H \\ &= \overline{(a \star b)}_H. \end{aligned}$$

### Théorème 2-3-9 :

Soient  $G$  un groupe abélien,  $H$  un sous-groupe de  $G$  et  $p$  la surjection canonique de  $G$  vers  $G/H$ .

- 1)  $G/H$  est une partie stable de  $\mathcal{P}(G)$  pour la loi induite.
- 2)  $G/H$  est un groupe abélien.
- 3) La surjection canonique  $p$  de  $G$  vers  $G/H$  est un homomorphisme de groupes.
- 4)  $\star$  est la seule loi de composition interne  $T$  dans  $G/H$  tel que  $p$  soit un homomorphisme de  $(G, \star)$  vers  $(G/H, T)$ .
- 5)  $\ker p = H$ .
- 6)  $p$  est un isomorphisme de  $G$  vers  $G/H$  si et seulement si  $H = \{e\}$ .

### Démonstration :

- 1)  $\forall x, y \in G/H : \exists a, b \in G \text{ tq } x = \overline{(a)}_H \text{ et } y = \overline{(b)}_H$ .

$$x \star y = \overline{(a)}_H \star \overline{(b)}_H = \overline{(a \star b)}_H \in G/H.$$

Donc  $G/H$  est une partie stable de  $\mathcal{P}(G)$  pour la loi induite.

- 2) • Puisque la loi  $\star$  est commutative dans  $\mathcal{P}(G)$  (car  $G$  est abélien) alors sa restriction à  $G/H$  est commutative.

• Puisque la loi  $\star$  est associative dans  $\mathcal{P}(G)$  alors sa restriction à  $G/H$  est associative.

- $\forall x \in G/H : \exists a \in G \text{ tq } x = \overline{(a)}_H$ .  $x \star \overline{(e)}_H = \overline{(a)}_H \star \overline{(e)}_H = \overline{(a \star e)}_H = \overline{(a)}_H = x$ .

Donc  $\overline{(e)}_H$  est l'élément neutre de  $G/H$ .

- Soit  $x$  un élément quelconque de  $G/H$ . Il existe alors il existe un élément de  $G$  tel que  $x = \overline{(a)}_H$ .

Soit  $a'$  le symétrique de  $a$  dans  $G$  pour la loi  $\star$ .

$$x \star \overline{(a')}_H = \overline{(a)}_H \star \overline{(a')}_H = \overline{(a \star a')}_H = \overline{(e)}_H.$$

Donc  $x$  est symétrisable pour la loi  $\star$  dans  $G/H$  dont le symétrique est égal à  $\overline{(a')}_H$ .

Ce qui montre que  $G/H$  est un groupe abélien.

$$3) \forall a, b \in G : p(a \star b) = \overline{(a \star b)}_H = \overline{(a)}_H \star \overline{(b)}_H = p(a) \star p(b).$$

Donc la surjection canonique  $p$  de  $G$  sur  $G/H$  est un homomorphisme de groupes.

4) Soit  $T$  une loi de composition interne quelconque dans  $G/H$  tel que  $p$  soit un homomorphisme de  $(G, \star)$  vers  $(G/H, T)$ .

$$\forall x, y \in G/H : \exists a, b \in G \text{ tq : } x = \overline{(a)}_H \text{ et } y = \overline{(b)}_H.$$

$$xTy = \overline{(a)}_H T \overline{(b)}_H = p(a)Tp(b) = p(a \star b) = p(a) \star p(b) = \overline{(a)}_H \star \overline{(b)}_H = x \star y.$$

Par suite  $T = \star$ . Donc  $\star$  est la seule loi de composition interne  $T$  dans  $G/H$  tel que  $p$  soit un homomorphisme de  $(G, \star)$  vers  $(G/H, T)$ .

$$5) \forall a \in G : a \in \ker p \Leftrightarrow p(a) = \overline{(e)}_H \Leftrightarrow \overline{(a)}_H = \overline{(e)}_H \Leftrightarrow a \star H = e \star H = H \Leftrightarrow a \in H.$$

Ce qui prouve que  $\ker p = H$ .

$$6) [p \text{ est un isomorphisme de } G \text{ vers } G/H] \Leftrightarrow p \text{ est injective} \Leftrightarrow \ker p = H \Leftrightarrow H = \{e\}.$$

### Théorème 2-3-10 :

Soient  $G$  et  $G'$  deux groupes (où  $G$  est abélien),  $f$  un homomorphisme de  $G$  vers  $G'$ ,  $H$  un sous-groupe de  $G$  et  $p$  la surjection canonique de  $G$  vers  $G/H$ .

Pour qu'il existe une application  $\overline{f}$  de  $G/H$  vers  $G'$  tel que :  $\overline{f} \circ p = f$  il faut et il suffit que :  $H \subset \ker f$ .

Dans ce cas :

- i)  $\overline{f}$  est unique.
- ii)  $\overline{f}$  est un homomorphisme de  $G/H$  vers  $G'$ .
- iii)  $\overline{f}$  est injectif si et seulement si  $H = \ker f$ .
- iv)  $\overline{f}$  est surjectif si et seulement si  $f$  est surjectif.

### Démonstration :

Soient  $\star$  la loi de  $G$ ,  $e$  l'élément neutre de  $G$  pour la loi de  $\star$ ,  $T$  la loi de  $G'$ ,  $\varepsilon$  l'élément neutre de  $G$  pour la loi de  $T$  et  $R$  la relation d'équivalence dans  $G$  définie par :

$$aRb \Leftrightarrow a' \star b \in H \text{ (où } a' \text{ est le symétrique de } a).$$

$R$  est la relation d'équivalence dans  $G$  associée à la partition  $G/H$  de  $G$ .

$\Rightarrow$  ) **Si  $\overline{f}$  existe :**

$$\forall a \in H : e' \star a = e \star a = a \in H \Rightarrow eRa \Rightarrow f(a) = f(e) = \varepsilon \text{ (car } \overline{f} \text{ existe)} \Rightarrow a \in \ker f.$$

$$\text{Donc : } H \subset \ker f.$$

$\Leftarrow$  ) **Si  $H \subset \ker f$  :**

Soient  $a$  et  $b$  deux éléments de  $G$  tels que  $aRb$ .

$$aRb \Rightarrow a' \star b \in H \subset \ker f \text{ (où } a' \text{ est le symétrique de } a) \Rightarrow f(a' \star b) = \varepsilon$$

$$\Rightarrow f(a') \star f(b) = \varepsilon \Rightarrow f(a)' \star f(b) = \varepsilon \text{ (où } f(a)' \text{ est le symétrique de } f(a))$$

$$\Rightarrow \overline{f}(a) = f(b).$$

Donc  $\overline{f}$  existe.

**Dans ce cas :**

i)  $\bar{f}$  est unique (d'après le théorème 2-3-10).

ii)  $\forall x, y \in G/H : \exists a, b \in G \text{ tq : } x = p(a) \text{ et } y = p(b).$

$$\begin{aligned}\bar{f}(x \star y) &= \bar{f}(p(a) \star p(b)) = \bar{f}(p(a \star b)) = (\bar{f} \circ p)(a \star b) = f(a \star b) \\ &= f(a) \star f(b) = (\bar{f} \circ p)(a) \star (\bar{f} \circ p)(b) = \bar{f}(p(a)) \star \bar{f}(p(b)) \\ &= \bar{f}(x) \star \bar{f}(y).\end{aligned}$$

Donc :  $\bar{f}$  est un homomorphisme de  $G/H$  vers  $G'$ .

iii)  $\Rightarrow$  ) **Si  $f$  est injectif :**

Puisque  $\bar{f}$  existe alors  $H \subset \ker f$ .

$\forall a \in \ker f : f(a) = \varepsilon = f(a) \Rightarrow eRa \Rightarrow a = e \star a = e' \star a \in H$ . Alors  $\ker f \subset H$ .

Donc  $H = \ker f$ .

$\Leftarrow$  ) **Si  $H = \ker f$  :**

$\forall a, b \in G :$

- Si  $aRb$  alors  $f(a) = f(b)$  (car  $\bar{f}$  existe).

- Si  $f(a) = f(b)$  alors :

$$f(a'b) = f(a')f(b) = f(a')f(b) = f(a')f(a) = \varepsilon \Rightarrow a'b \in \ker f = H \Rightarrow aRb.$$

Alors :  $aRb \Leftrightarrow f(a) = f(b)$ .

Donc  $f$  est injectif.

iv)  $\bar{f}$  est surjectif si et seulement si  $f$  est surjectif (d'après le théorème 2-3-10).

**Corolaire 2-3-11 :**

Soient  $G$  et  $G'$  deux groupes (où  $G$  est abélien).  $f$  un homomorphisme de  $G$

Si  $f$  est un homomorphisme de  $G$  vers  $G'$  alors  $G/\ker f$  est isomorphe à  $f(G)$ .

C'est à dire si  $f$  est un homomorphisme de  $G$  vers  $G'$  alors :  $G/\ker f \simeq f(G)$ .

**Démonstration :**

Soit  $f$  un homomorphisme de  $G$  vers  $G'$  et posons  $H = \ker f$ .

$f$  est un homomorphisme surjectif de  $G$  vers  $f(G)$ .

Puisque  $H = \ker f$  alors (d'après le théorème 2-3-10) il existe un homomorphisme injectif  $\bar{f}$  de  $G/H$  vers  $f(G)$  tel que  $\bar{f} \circ p = f$  (où  $p$  est la surjection canonique de  $G$  vers  $G/H$ ).

Donc  $\bar{f}$  est un isomorphisme de  $G/H = G/\ker f$  vers  $f(G)$ .

Ce qui montre que :  $G/\ker f = G/H \simeq f(G)$ .

**Corolaire 2-3-12 :**

Soient  $G$  et  $G'$  deux groupes abéliens ,  $f$  un homomorphisme de  $G$  vers  $G'$ ,

$H$  et  $H'$  deux sous-groupes respectivement de  $G$  et  $G'$ ,  $p$  la surjection canonique de  $G$  vers  $G/H$  et  $p'$  la surjection canonique de  $G'$  vers  $G'/H'$ .

Pour qu'il existe une application  $\bar{f}$  de  $G/H$  vers  $G'/H'$  tel que :  $\bar{f} \circ p = p' \circ f$  il faut et il suffit que :  $H \subset f^{-1}(H')$ .

**Dans ce cas :**

i)  $\bar{f}$  est unique.

ii)  $\bar{f}$  est un homomorphisme de  $G/H$  vers  $G'/H'$ .

iii)  $\bar{f}$  est injectif si et seulement si  $H = f^{-1}(H')$ .

iv) Si  $f$  est surjectif alors  $\bar{f}$  est surjectif.



**Démonstration :**

Soit  $e'$  l'élément neutre de  $G'$  et posons  $\varphi = p' \circ f$ .

$(e')_{H'} = H'$  est l'élément neutre de  $G'/H'$  et  $\varphi$  est un homomorphisme de  $G$  vers  $G'/H'$ .

Pour qu'il existe une application  $\bar{f}$  de  $G/H$  vers  $G'/H'$  tel que :  $\bar{f} \circ p = \varphi = p' \circ f$  il faut et il suffit que  $H \subset \ker \varphi$  (d'après le théorème 2-3-10).

$$\begin{aligned} \forall a \in \ker \varphi &\Leftrightarrow \varphi(a) = (e')_{H'} \Leftrightarrow (p' \circ f)(a) = H' \Leftrightarrow p'(f(a)) = H' \Leftrightarrow \overline{(f(a))}_{H'} = H' \\ &\Leftrightarrow f(a) \in H' \\ &\Leftrightarrow a \in f^{-1}(H'). \end{aligned}$$

Donc :  $\ker \varphi = f^{-1}(H')$ .

Ce qui montre que l'application  $\bar{f}$  existe si et seulement si  $H \subset f^{-1}(H')$ .

**Dans ce cas :**

- i)  $\bar{f}$  est unique (d'après le théorème 2-3-10).
- ii)  $\bar{f}$  est un homomorphisme de  $G/H$  vers  $G'/H'$  (d'après le théorème 2-3-10).
- iii)  $\bar{f}$  est injectif si et seulement si  $H = \ker \varphi = f^{-1}(H')$ .
- iv) Supposons que  $f$  est surjectif.  
Alors  $p' \circ f$  est surjectif, et par suite  $\bar{f} \circ p = p' \circ f$  est surjectif.  
Donc  $\bar{f}$  est surjectif.

**Remarque 2-3-13 :**

Si  $G$  est un groupe abélien et si  $e$  est son élément neutre alors  $G/\{e\} \simeq G$ .

En particulier  $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \simeq \mathbb{Z}$ .

**En effet :**

$$G/\{e\} = G/\ker(\text{id}_G) \simeq \text{id}_G(G) = G.$$

$$\text{En particulier } \mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \simeq \mathbb{Z}.$$

**2-4 - Sous-groupes engendrés :****Proposition et définition 2-4-1 :**

Soient  $G$  un groupe et  $S$  une partie de  $G$ .

L'ensemble  $\mathcal{M}$  des sous-groupes de  $G$  contenant  $S$  n'est pas vide (car  $S \in \mathcal{M}$ ).

L'intersection des éléments de  $\mathcal{M}$  est le plus petit (pour l'inclusion) élément de  $\mathcal{M}$  appelé le sous-groupe de  $G$  engendré par  $S$  et noté  $\langle S \rangle$

Si  $a \in G$  et si  $S = \{a\}$  alors :

- $\langle \{a\} \rangle$  est noté  $\langle a \rangle$ . C'est à dire :  $\langle a \rangle = \langle \{a\} \rangle$
- Si  $\langle a \rangle$  est d'ordre fini  $n$  on dit aussi que  $a$  est d'ordre fini  $n$  et on note  $|a| = n$ .
- Si  $\langle a \rangle$  est d'ordre infini on dit aussi que  $a$  est d'ordre infini.

**Propriétés 2-4-2 :**

Soient  $(G, *)$  un groupe,  $e$  son élément neutre et  $S$  une partie de  $G$ .

1)  $S \subset \langle S \rangle$ .

2) Si  $H$  est un sous-groupe de  $G$  alors  $\langle S \rangle \subset H$  si et seulement si  $S \subset H$ .

3) Si  $H$  est un sous-groupe de  $G$  alors  $\langle H \rangle = H$ .

4)  $\langle \emptyset \rangle = \langle e \rangle = \{e\}$ .

5) Si  $S \neq \emptyset$ .

a) L'ensemble  $\{x_1 * x_2 * \dots * x_n \mid tq : x_1, x_2, \dots, x_n \in S \cup S'\}$   
(où  $S'$  est l'ensemble des symétriques des éléments de  $S$ ) est un sos-groupe de  $G$  contenant  $S$ .

b)  $\langle S \rangle = \{x_1 * x_2 * \dots * x_n \mid tq : x_1, x_2, \dots, x_n \in S \cup S'\}$   
où  $S'$  est l'ensemble des symétriques des éléments de  $S$ .

6) Si  $G$  est multiplicatif alors :

$\forall a \in G : \langle a \rangle = \{a^k \mid tq : k \in \mathbb{Z}\}$  qui est un sous-groupe abélien de  $G$

7) Si  $G$  est additif alors :

$\forall a \in G : \langle a \rangle = \{ka \mid tq : k \in \mathbb{Z}\}$  qui est un sous-groupe abélien de  $G$

### Démonstration :

1) Puisque  $\langle S \rangle$  est le plus petit (pour l'inclusion) sos-groupe de  $G$  contenant  $S$  alors  $S \subset \langle S \rangle$ .

2) Soit  $H$  un sous-groupe de  $G$ .

$\Rightarrow$  ) **Si**  $\langle S \rangle \subset H$  :

Alors :  $S \subset \langle S \rangle \subset H$ . Donc :  $S \subset H$ .

$\Leftarrow$  ) **Si**  $S \subset H$  :

Soit  $\mathcal{M}$  l'ensemble des sous groupes de  $G$  contenant  $S$ .

Puisque  $S \subset H$  alors  $H \in \mathcal{M}$ .

Donc  $\langle S \rangle \subset H$  (car  $\langle S \rangle$  est le plus petit élément de  $\mathcal{M}$ ).

3) Soit  $H$  un sous-groupe de  $G$ .

D'après 1) on a :  $H \subset \langle H \rangle$ .

Puisque  $H \subset H$  et puisque  $H$  est un sous-groupe de  $G$  alors (d'après 2))  $\langle H \rangle \subset H$ .

Donc  $\langle H \rangle = H$ .

4)  $\emptyset \subset \{e\} \Rightarrow \langle \emptyset \rangle \subset \{e\}$  (car  $\{e\}$  est un sos-groupe de  $G$ ).

Puisque  $\langle \emptyset \rangle$  est un sos-groupe de  $G$  alors :  $e \in \langle \emptyset \rangle \Rightarrow \{e\} \subset \langle \emptyset \rangle$ .

Donc  $\langle \emptyset \rangle = \{e\}$ . On a aussi  $\langle e \rangle = \langle \{e\} \rangle = \{e\}$  (car  $\{e\}$  est un sos-groupe de  $G$ ).

Par suite on a :  $\langle \emptyset \rangle = \langle e \rangle = \{e\}$ .

5) Supposons que  $S \neq \emptyset$ .

a) Posons  $H = \{x_1 * x_2 * \dots * x_n \mid tq : x_1, x_2, \dots, x_n \in S \cup S'\}$

où  $S'$  est l'ensemble des symétriques des éléments de  $S$ .

• Soit  $x$  un élément quelconque de  $S$ .

Posons  $x_1 = x$ ,  $x_2$  le symétrique de  $x$  et  $x_3 = x$  alors :

$x_1, x_2, x_3 \in S \cup S'$  et  $x = e * x = x_1 * x_2 * x_3 \in H$ .

Donc :  $S \subset H$ .

•  $[S \neq \emptyset \text{ et } S \subset H] \Rightarrow H \neq \emptyset$ .

•  $\forall x, y \in H : \exists x_1, \dots, x_n, y_1, \dots, y_m \in S \cup S' \text{ tq : } \begin{cases} x = x_1 * \dots * x_n \\ y = y_1 * \dots * y_m \end{cases}$ .

$\forall i = 1, \dots, n, n+1, \dots, n+m$ , posons :  $\begin{cases} z_i = x_i & \text{si } i = 1, \dots, n \\ z_i = y_{i-n} & \text{si } i = n+1, \dots, n+m \end{cases}$ .

$z_1, \dots, z_n, z_{n+1}, \dots, z_{n+m} \in S \cup S'$ .

Donc :  $x * y = (x_1 * \dots * x_n) * (y_1 * \dots * y_m)$

$= z_1 * \dots * z_n * z_{n+1} * \dots * z_{n+m} \in H$ .

Donc  $H$  est stable pour la loi  $*$ .

- $\forall x \in H : \exists x_1, \dots, x_n \in S \cup S' \text{ tq : } x = x_1 * \dots * x_n.$

Pousons  $x'$  le symétrique de  $x$ .

$\forall i = 1, \dots, n$ , posons :  $x'_i$  le symétrique de  $x_i$ .  $x'_1, \dots, x'_n \in S \cup S'$ .

$x' = (x_1 * \dots * x_n)' = x'_n * \dots * x'_1 \in H$ .

Ce qui montre que  $\{x_1 * \dots * x_n \text{ tq : } x_1, \dots, x_n \in S \cup S'\} = H$  est un sos-groupe de  $G$  contenant  $S$ .

b) Posons  $H = \{x_1 * \dots * x_n \text{ tq : } x_1, x_2, \dots, x_n \in S \cup S'\}$

où  $S'$  est l'ensemble des symétriques des éléments de  $S$ .

- Puisque  $H$  est un sos-groupe de  $G$  contenant  $S$  alors  $\langle S \rangle \subset H$ .

- Soit  $x$  un élément quelconque de  $H$ .

Il existe alors  $x_1, x_2, \dots, x_n \in S \cup S'$  tels que :  $x = x_1 * \dots * x_n$ .

$\forall i = 1, \dots, n$ , posons :  $x'_i$  le symétrique de  $x_i$ .

$\forall i = 1, \dots, n$  :

- Si  $x_i \in S : x_i \in S \subset \langle S \rangle$ .

- Si  $x_i \in S' : x_i \in S' \Rightarrow x'_i \in S \subset \langle S \rangle \Rightarrow x_i \in \langle S \rangle$ .

Donc :  $x_1, x_2, \dots, x_n \in \langle S \rangle \Rightarrow x = x_1 * \dots * x_n \in \langle S \rangle$ .

Par suite  $H \subset \langle S \rangle$ .

Ce qui prouve que :  $\langle S \rangle = H = \{x_1 * \dots * x_n \text{ tq : } x_1, x_2, \dots, x_n \in S \cup S'\}$ .

6) Supposons que  $G$  est multiplicatif et soit  $a$  un élément quelconque de  $G$ .

Posons  $H = \{a^k \text{ tq : } k \in \mathbb{Z}\}$ .  $H$  est un sous-groupe abélien de  $G$ .

- $a = a^1 \in H \Rightarrow \langle a \rangle \subset H$ . (car  $H$  est un sous-groupe de  $G$  contenant  $a$ ).

- Montrons que  $H \subset \langle a \rangle$ .

★ Montrons par récurrence que pour tout entier naturel  $k$ ,  $a^k \in \langle a \rangle$ .

- Pour  $k = 1$  :

$a^k = a^0 = e \in \langle a \rangle$ .

- Pour  $k - 1$  :

Supposons que  $a^{k-1} \in \langle a \rangle$ .

- Pour  $k$  :

Montrons qu'alors  $a^k \in \langle a \rangle$ .

$a^k = a^{k-1}a \in \langle a \rangle$ . (ca  $\langle a \rangle$  est un sous-groupe de  $G$ ).

On a alors monter que pour tout entier naturel  $k$ ,  $a^k \in \langle a \rangle$ .

★ Montrons que pour tout entier relatif  $k$ ,  $a^k \in \langle a \rangle$ .

Soit  $k$  un entier relatif quelconque.

- Si  $k \geq 0$  :

Alors :  $k \in \mathbb{N} \Rightarrow a^k \in \langle a \rangle$ .

- Si  $k \leq 0$  :

Alors :  $-k \geq 0 \Rightarrow a^{-k} \in \langle a \rangle \Rightarrow a^k = (a^{-k})^{-1} \in \langle a \rangle$ .

★  $\forall x \in H : \exists k \in \mathbb{Z} \text{ tq : } x = a^k \in \langle a \rangle$ .

Donc :  $H \subset \langle a \rangle$ .

Ce qui montre que  $\langle a \rangle = H = \{a^k \text{ tq : } k \in \mathbb{Z}\}$  qui est un sous-groupe abélien de  $G$ .

7) Supposons que  $G$  est additif et soit  $a$  un élément quelconque de  $G$ .

Posons  $H = \{ka \text{ tq : } k \in \mathbb{Z}\}$ .  $H$  est un sous-groupe abélien de  $G$ .

- $a = 1a \in H \Rightarrow \langle a \rangle \subset H$ . (car  $H$  est un sous-groupe de  $G$  contenant  $a$ ).

- Montrons que  $H \subset \langle a \rangle$ .
    - ★ Montrons par récurrence que pour tout entier naturel  $k$ ,  $ka \in \langle a \rangle$ .
      - **Pour  $k = 1$  :**  
 $ka = 0a = 0_G \in \langle a \rangle$ .
      - **Pour  $k - 1$  :**  
 Supposons que  $(k - 1)a \in \langle a \rangle$ .
      - **Pour  $k$  :**  
 Montrons qu'alors  $ka \in \langle a \rangle$ .  
 $ka = (k - 1)a + a \in \langle a \rangle$ . (car  $\langle a \rangle$  est un sous-groupe de  $G$ ).  
 On a alors montré que pour tout entier naturel  $k$ ,  $ka \in \langle a \rangle$ .
    - ★ Montrons que pour tout entier relatif  $k$ ,  $ka \in \langle a \rangle$ .  
 Soit  $k$  un entier relatif quelconque.
      - **Si  $k \geq 0$  :**  
 Alors :  $k \in \mathbb{N} \Rightarrow ka \in \langle a \rangle$ .
      - **Si  $k \leq 0$  :**  
 Alors :  $-k \geq 0 \Rightarrow (-k)a \in \langle a \rangle \Rightarrow a^k = -[(-k)a] \in \langle a \rangle$ .
    - ★  $\forall x \in H : \exists k \in \mathbb{Z} \text{ tq } x = ka \in \langle a \rangle$ .  
 Donc :  $H \subset \langle a \rangle$ .
- Ce qui montre que  $\langle a \rangle = H = \{ka \text{ tq } k \in \mathbb{Z}\}$  qui est un sous-groupe abélien de  $G$ .

### Exemple 2-4-3 :

Pour tout entier relatif  $n$ ,  $\langle n \rangle = n\mathbb{Z}$ . C'est à dire,  $\forall n \in \mathbb{Z} : \langle n \rangle = n\mathbb{Z}$ .  
 En particulier :  $\langle 0 \rangle = 0\mathbb{Z} = \{0\}$ ,  $\langle 1 \rangle = 1\mathbb{Z} = \mathbb{Z}$  et  $\langle -1 \rangle = (-1)\mathbb{Z} = \mathbb{Z}$ .

### En effet :

$\forall n \in \mathbb{Z} : \langle n \rangle = \{kn \text{ tq } k \in \mathbb{Z}\} = \{nk \text{ tq } k \in \mathbb{Z}\} = n\mathbb{Z}$ .  
 En particulier :  $\langle 0 \rangle = 0\mathbb{Z} = \{0\}$ ,  $\langle 1 \rangle = 1\mathbb{Z} = \mathbb{Z}$  et  $\langle -1 \rangle = (-1)\mathbb{Z} = \mathbb{Z}$ .

### Théorème 2-4-4 :

Soient  $G$  et  $G'$  deux groupes et  $f$  un homomorphisme de  $G$  vers  $G'$ .  
 Si  $S$  est une partie de  $G$  alors :  $f(\langle S \rangle) = \langle f(S) \rangle$ .

### Démonstration :

Soient  $S$  une partie de  $G$ ,  $\star$  la loi de  $G$ ,  $T$  la loi de  $G'$ ,  $e$  l'élément neutre de  $G$  et  $\varepsilon$  l'élément neutre de  $G'$ .

- **Si  $S = \emptyset$  :**  
 $f(\langle S \rangle) = f(\langle \emptyset \rangle) = f(\{e\}) = \{f(e)\} = \{\varepsilon\} = \langle \emptyset \rangle = \langle f(\emptyset) \rangle = \langle f(S) \rangle$ .
- **Si  $S \neq \emptyset$  :**  
 ⊂ ) Posons  $f(S)'$  l'ensemble des symétriques des éléments de  $f(S)$ .  
 Soit  $y$  un élément quelconque de  $f(\langle S \rangle)$ .  
 Il existe alors un élément  $x$  de  $\langle S \rangle$  tel que  $y = f(x)$ .  
 $x \in \langle S \rangle \Rightarrow \exists x_1, \dots, x_n \in S \cup S' \text{ tq } x = x_1 \star \dots \star x_n$ .  
 $y = f(x_1 \star \dots \star x_n) = f(x_1)T \dots Tf(x_n)$ .  
 $\forall i = 1, \dots, n$ , posons :  $x'_i$  le symétrique de  $x_i$   
 $\forall i = 1, \dots, n$  :

- Si  $\mathbf{x}_i \in \mathbf{S} : x_i \in S \Rightarrow f(x_i) \in f(S) \subset f(S) \cup f(S)'$ .
- Si  $\mathbf{x}_i \in \mathbf{S}' : x'_i \in S \Rightarrow f(x'_i) \in f(S) \Rightarrow f(x_i) \in f(S)' \subset f(S) \cup f(S)'$   
(car  $f(x'_i)$  est le symétrique de  $f(x_i)$ ).

Alors :  $f(x_1), \dots, f(x_n) \in f(S) \cup f(S)'$ .

Donc :  $y = f(x_1 * \dots * x_n) = f(x_1)T \dots Tf(x_n) \in \langle f(S) \rangle$ .

Par suite on a :  $f(\langle S \rangle) \subset \langle f(S) \rangle$

$\Rightarrow S \subset \langle S \rangle \Rightarrow f(S) \subset f(\langle S \rangle) \Rightarrow \langle f(S) \rangle \subset f(\langle S \rangle)$  (car  $f(\langle S \rangle)$  est un sous-groupe de  $G'$ ).

Ce qui montre que  $f(\langle S \rangle) = \langle f(S) \rangle$ .

### Corolaire 2-4-5 :

Soient  $G$  et  $G'$  deux groupes et  $f$  un homomorphisme de  $G$  vers  $G'$ .

Pour tout élément  $a$  de  $G$ ,  $f(\langle a \rangle) = \langle f(a) \rangle$ . C'est à dire :  $\forall a \in G : f(\langle a \rangle) = \langle f(a) \rangle$ .

**En effet :**

$$\forall a \in G : f(\langle a \rangle) = f(\langle \{a\} \rangle) = \langle f(\{a\}) \rangle = \langle \{f(a)\} \rangle = \langle f(a) \rangle.$$

### Exemple 2-4-6 :

Pour tout entier naturel  $n$ ,  $\langle \bar{1} \text{ (modulo } n) \rangle = \mathbb{Z}/n\mathbb{Z}$ .

C'est à dire :  $\forall n \in \mathbb{N} : \langle \bar{1} \text{ (modulo } n) \rangle = \mathbb{Z}/n\mathbb{Z}$ .

**En effet :**

Soient  $n$  un entier naturel quelconque et  $p$  la surjection canonique de  $\mathbb{Z}$  vers  $\mathbb{Z}/n\mathbb{Z}$ .

$$\langle \bar{1} \text{ (modulo } n) \rangle = \langle p(1) \rangle = p(\langle 1 \rangle) = p(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

### Théorème 2-4-7 :

Soient  $G$  un groupe (en général multiplicatif),  $e$  son élément neutre,  $a \in G$  un élément quelconque de  $G$  et  $f$  l'homomorphisme de  $\mathbb{Z}$  vers  $G$  défini par :

$$f : \mathbb{Z} \rightarrow G$$

$$k \mapsto f(k) = a^k \text{ (dans le cas additif } f(k) = ka).$$

Soit  $n$  l'entier naturel tel que :  $\ker f = n\mathbb{Z}$ .

On a les propriétés suivantes :

- 1)  $\langle a \rangle \simeq \mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z}$
- 2)  $a$  est d'ordre fini si et seulement si  $n \neq 0$  et dans ce cas  $a$  est d'ordre  $n$ .
- 3)  $a$  est d'ordre infini si et seulement si  $n = 0$  et dans ce cas :  $\langle a \rangle \simeq \mathbb{Z}$ .
- 4)  $n\mathbb{Z} = \{k \in \mathbb{Z} \text{ tq : } a^k = e\}$  (dans le cas additif :  $n\mathbb{Z} = \{k \in \mathbb{Z} \text{ tq : } ka = 0_G\}$ ).
- 5) Les 3 propriétés suivantes sont équivalents :
  - i)  $a$  est d'ordre fini.
  - ii)  $\exists k \in \mathbb{N}^* \text{ tq : } a^k = e$  (dans le cas additif :  $\exists k \in \mathbb{N}^* \text{ tq : } ka = 0_G$ ).
  - iii)  $\exists k \in \mathbb{Z}^* \text{ tq : } a^k = e$  (dans le cas additif :  $\exists k \in \mathbb{Z}^* \text{ tq : } ka = 0_G$ ).
- 6) Si  $a$  est d'ordre fini.
  - i)  $|a|$  est le plus petit entier naturel non nul  $k$  tel que  $a^k = e$ .  
Dans le cas additif :  
 $|a|$  est le plus petit entier naturel non nul  $k$  tel que  $ka = 0_G$ .
  - ii)  $\forall k \in \mathbb{Z} : a^k = e \Leftrightarrow |a| \mid k$  (dans le cas additif :  $\forall k \in \mathbb{Z} : ka = 0_G \Leftrightarrow |a| \mid k$ ).

7) Les trois propriétés suivantes sont équivalents :

- i)  $a$  est d'ordre infini.
- ii)  $\forall k \in \mathbb{Z}^* : a^k \neq e$  (dans le cas additif :  $\forall k \in \mathbb{Z}^* : ka \neq 0_G$ ).
- iii)  $\forall k \in \mathbb{N}^* : a^k \neq e$  (dans le cas additif :  $\forall k \in \mathbb{N}^* : ka \neq 0_G$ ).

**Démonstration :**

$$1) \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} \text{ (dans le cas additif } \langle a \rangle = \{ka \mid k \in \mathbb{Z}\}) \\ = \{f(k) \mid k \in \mathbb{Z}\} = f(\mathbb{Z}) \\ \simeq \mathbb{Z} / \ker f = \mathbb{Z} / n\mathbb{Z}$$

$$2) [a \text{ est d'ordre fini}] \Leftrightarrow [\mathbb{Z}/n\mathbb{Z} \text{ est d'ordre fini}] \Leftrightarrow n \neq 0.$$

**Dans ce cas :**  $|a| = |\langle a \rangle| = |\mathbb{Z}/n\mathbb{Z}| = n$ .

$$3) [a \text{ est d'ordre infini}] \Leftrightarrow [\mathbb{Z}/n\mathbb{Z} \text{ est d'ordre infini}] \Leftrightarrow n = 0.$$

$$4) n\mathbb{Z} = \ker f = \{k \in \mathbb{Z} \mid f(k) = e\} = \{k \in \mathbb{Z} \mid a^k = e\}.$$

**Dans le cas additif :**

$$n\mathbb{Z} = \ker f = \{k \in \mathbb{Z} \mid f(k) = 0_G\} = \{k \in \mathbb{Z} \mid ka = 0_G\}.$$

5) • Supposons que  $a$  est d'ordre fini.

Alors  $n \neq 0$ . Donc :  $n \in \mathbb{N}^*$  et  $n \in \{k \in \mathbb{Z} \mid a^k = e\}$ .

Pour  $k = n$  on a alors  $a^k = a^n = e$ . Par suite il existe  $k \in \mathbb{N}^* \mid a^k = e$ .

Ce qui prouve que i)  $\Rightarrow$  ii) est vraie.

**Dans le cas additif :**

Supposons que  $a$  est d'ordre fini.

Alors  $n \neq 0$ . Donc :  $n \in \mathbb{N}^*$  et  $n \in \{k \in \mathbb{Z} \mid ka = 0_G\}$ .

Pour  $k = n$  on a alors  $ka = na = 0_G$ . Par suite il existe  $k \in \mathbb{N}^* \mid ka = 0_G$ .

Ce qui prouve que i)  $\Rightarrow$  ii) est vraie.

• ii)  $\Rightarrow$  iii) est vraie (car  $\mathbb{N}^* \subset \mathbb{Z}^*$ ).

• Supposons qu'il existe  $k \in \mathbb{Z}^* \mid a^k = e$ .

Alors :  $n\mathbb{Z} = \{k \in \mathbb{Z} \mid a^k = e\} \neq \{0\} = 0\mathbb{Z} \Rightarrow n \neq 0$ .

Donc  $a$  est d'ordre fini.

Par suite iii)  $\Rightarrow$  i) est vraie.

**Dans le cas additif :**

Supposons qu'il existe  $k \in \mathbb{Z}^* \mid ka = 0_G$ .

Alors :  $n\mathbb{Z} = \{k \in \mathbb{Z} \mid ka = 0_G\} \neq \{0\} = 0\mathbb{Z} \Rightarrow n \neq 0$ .

Donc  $a$  est d'ordre fini.

Par suite iii)  $\Rightarrow$  i) est vraie.

Ce qui montre que les 3 propriétés i), ii) et iii) sont équivalents.

6) Supposons que  $a$  est d'ordre fini.

i) Alors  $n = |a| \in \mathbb{N}^*$  est le plus petit entier naturel non nul de  $n\mathbb{Z}$ .

Puisque  $\{k \in \mathbb{Z} \mid a^k = e\} = n\mathbb{Z}$  alors  $|a| = n$  est le plus petit entier naturel non nul de  $\{k \in \mathbb{Z} \mid a^k = e\}$ .

Ce qui prouve que  $|a|$  est le plus petit entier naturel non nul  $k$  tel que  $a^k = e$ .

**Dans le cas additif :**

$|a|$  est le plus petit entier naturel non nul  $k$  tel que  $ka = 0_G$ .

$$\text{ii) } \forall k \in \mathbb{Z} : a^k = e \Leftrightarrow f(k) = e \Leftrightarrow k \in \ker f \Leftrightarrow k \in n\mathbb{Z} \Leftrightarrow n|k \Leftrightarrow |a||k|$$

**Dans le cas additif :**

$$\forall k \in \mathbb{Z} : ka = 0_G \Leftrightarrow f(k) = 0_G \Leftrightarrow k \in \ker f \Leftrightarrow k \in n\mathbb{Z} \Leftrightarrow n|k \Leftrightarrow |a||k|$$

7) Puisque les trois propriétés i), ii) et iii) sont les négations des trois propriétés de 6), alors les trois propriétés i), ii) et iii) sont équivalents.

**Corollaire 2-4-8 :**

Soenit  $(G, .)$  un groupe d'ordre fini  $n$  et  $e$  son élément neutre.

Pour tout élément  $a$  de  $G$  on a :  $a^n = e$  (dans le cas additif :  $na = 0_G$ ).

**En effet :**

Soit  $a$  un élément de  $G$ .

Puisque  $G$  est d'ordre fini et puisque  $\langle a \rangle$  est un sous-groupe de  $G$  alors  $\langle a \rangle$  est d'ordre fini et que son ordre est un diviseur de l'ordre de  $G$ .

Donc  $|a| = |\langle a \rangle|$  est un diviseur de  $|G| = n$ .

Ce qui montre (d'après la propriété 6) du théorème 2-4-7) que  $a^n = e$ .

**Dans le cas additif on a :**  $na = 0_G$ .

**Corollaire 2-4-9 :**

Soenit  $(G, .)$  un groupe et  $a, b \in G$ . Si  $a$  et  $b$  vérifie les trois propriétés suivantes :

1)  $a$  et  $b$  sont d'ordres finis.

2)  $ab = ba$  (dans le cas additif :  $a + b = b + a$ ).

3)  $\langle a \rangle \cap \langle b \rangle = \{e\}$  (dans le cas additif :  $\langle a \rangle \cap \langle b \rangle = \{0_G\}$ ).

alors  $ab$  est d'ordre fini et  $|ab| = |a| \vee |b|$  (dans le cas additif :  $|a + b| = |a| \vee |b|$ ).

**Démonstration :**

$(ab)^{|a| \vee |b|} = a^{|a| \vee |b|} b^{|a| \vee |b|} = ee = e$ . Donc  $ab$  est d'ordre fini et son ordre divise  $|a| \vee |b|$ .

Posons  $|ab| = r$ .

Alors :  $(ab)^r = e \Rightarrow a^r b^r = e \Rightarrow a^r = b^{-r} \in \langle a \rangle \cap \langle b \rangle = \{e\} \Rightarrow a^r = b^{-r} = e$   
 $\Rightarrow a^r = b^r = e \Rightarrow (|a||r \text{ et } |b||r) \Rightarrow (|a| \vee |b|)|r$ .

Ce qui montre que :  $|ab| = r = |a| \vee |b|$ .

**Dans le cas additif :**

$(|a| \vee |b|)(a + b) = (|a| \vee |b|)a + (|a| \vee |b|)b = 0_G + 0_G = 0_G$ .

Donc  $a + b$  est d'ordre fini et son ordre divise  $|a| \vee |b|$ .

Posons  $|a + b| = r$ .

Alors :  $r(a + b) = 0_G \Rightarrow ra + rb = 0_G \Rightarrow ra^r = -rb = (-r)b \in \langle a \rangle \cap \langle b \rangle = \{e\}$   
 $\Rightarrow ra^r = -rb = e \Rightarrow ra = rb = e \Rightarrow (|a||r \text{ et } |b||r)$   
 $\Rightarrow (|a| \vee |b|)|r$ .

Ce qui montre que :  $|a + b| = r = |a| \vee |b|$ .

**Corollaire 2-4-10 :**

Soenit  $(G, .)$  un groupe et  $a, b \in G$ . Si  $a$  et  $b$  vérifie les trois propriétés suivantes :

1)  $a$  et  $b$  sont d'ordres finis.

2)  $ab = ba$  (dans le cas additif :  $a + b = b + a$ ).

3)  $|a| \wedge |b| = 1$ .

alors  $ab$  est d'ordre fini et  $|ab| = |a||b|$  (dans le cas additif :  $|a + b| = |a||b|$ ).

**Démonstration :**

$\forall u \in \langle a \rangle \cap \langle b \rangle : \begin{cases} u \in \langle a \rangle \\ u \in \langle b \rangle \end{cases} \Rightarrow \begin{cases} |u||a| \\ |u||b| \end{cases} \Rightarrow |u|(|a| \wedge |b|) \Rightarrow |u|1 \Rightarrow |u| = 1$   
 $\Rightarrow u = e$  (dans le cas additif :  $u = 0_G$ ).

Donc :  $\langle a \rangle \cap \langle b \rangle = \{e\}$  (dans le cas additif :  $\langle a \rangle \cap \langle b \rangle = \{0_G\}$ ).

Ce qui montre (d'après la propriété précédente) que  $ab$  est d'ordre fini et  $|ab| = |a| \vee |b| = |a||b|$ .

**Dans le cas additif :**  $a + b$  est d'ordre fini et  $|a + b| = |a| \vee |b| = |a||b|$ .

**Corollaire 2-4-11 :**

Soient  $(G, \cdot)$  un groupe et  $a$  un élément de  $G$  d'ordre fini.

Pour tout entier relatif  $k$ ,  $a^k$  est d'ordre fini et  $|a^k| = \frac{|a|}{k \wedge |a|}$ .

$$\text{C'est à dire : } \forall k \in \mathbb{Z} : \begin{cases} a^k \text{ est d'ordre fini} \\ |a^k| = \frac{|a|}{k \wedge |a|} \end{cases}.$$

**Dans le cas additif :**

Pour tout entier relatif  $k$ ,  $ka^k$  est d'ordre fini et  $|ka| = \frac{|a|}{k \wedge |a|}$ .

$$\text{C'est à dire : } \forall k \in \mathbb{Z} : \begin{cases} ka \text{ est d'ordre fini} \\ |ka| = \frac{|a|}{k \wedge |a|} \end{cases}.$$

**Démonstration :**

Soient un entier relatif quelconque  $k$ .

Puisque  $a$  est d'ordre fini et puisque  $a^k \in \langle a \rangle$  (dans le cas multiplicatif  $ka \in \langle a \rangle$ ) alors  $a^k$  est d'ordre fini (dans le cas multiplicatif  $ka$  est d'ordre fini).

Posons :  $|a| = n$  et  $|a^k| = r$  (dans le cas multiplicatif  $|ka| = r$ ).

$(a^k)^r = e \Rightarrow a^{kr} = e \Rightarrow n|kr \Rightarrow \exists l \in \mathbb{Z} \text{ tq : } kr = ln.$

$$\text{Posons : } n \wedge k = d. \text{ Alors : } \exists n_0, k_0 \in \mathbb{Z} \text{ tq : } \begin{cases} n = n_0 d \\ k = k_0 d \\ n_0 \wedge k_0 = 1 \end{cases}$$

Par suite  $k_0 dr = ln_0 d \Rightarrow k_0 r = ln_0$  ( $d \neq 0$  car  $n \neq 0$ ). Alors :

$$\begin{cases} n_0 \neq 0 \\ n_0 | k_0 r \\ n_0 \wedge k_0 = 1 \end{cases} \Rightarrow n_0 | r.$$

De même on a :  $(a^k)^{n_0} = a^{kn_0} = a^{k_0 dn_0} = a^{k_0 n} = e \Rightarrow r | n_0$ .

Ce qui montre que :  $|a^k| = r = n_0 = \frac{n}{d} = \frac{n}{k \wedge n} = \frac{|a|}{k \wedge |a|}$ .

**Dans le cas additif :**

$r(ka) = 0_G \Rightarrow (rk)a = 0_G \Rightarrow n|kr \Rightarrow \exists l \in \mathbb{Z} \text{ tq : } kr = ln.$

$$\text{Posons : } n \wedge k = d. \text{ Alors : } \exists n_0, k_0 \in \mathbb{Z} \text{ tq : } \begin{cases} n = n_0 d \\ k = k_0 d \\ n_0 \wedge k_0 = 1 \end{cases}$$

Par suite  $k_0 dr = ln_0 d \Rightarrow k_0 r = ln_0$  ( $d \neq 0$  car  $n \neq 0$ ). Alors :

$$\begin{cases} n_0 \neq 0 \\ n_0 | k_0 r \\ n_0 \wedge k_0 = 1 \end{cases} \Rightarrow n_0 | r.$$



De même on a :  $n_0(ka) = (n_0k)a = (n_0dk_0)a = (k_0n_0d)a = (k_0n)a = 0_G \Rightarrow r|n_0$ .

Ce qui montre que :  $|ka| = r = n_0 = \frac{n}{d} = \frac{n}{k \wedge n} = \frac{|a|}{k \wedge |a|}$ .

### Exemple 2-4-12 :

Pour tout entier naturel non nul  $n \in \mathbb{N}^*$  et pour tout entier relatif  $k$ ,

$$|\bar{k} \text{ (modulo } n)| = \frac{n}{k \wedge n}.$$

C'est à dire :  $\forall n \in \mathbb{N}^*$  et  $\forall k \in \mathbb{Z} : |\bar{k} \text{ (modulo } n)| = \frac{n}{k \wedge n}$ .

### En effet :

$$\begin{aligned} \forall n \in \mathbb{N}^* \text{ et } \forall k \in \mathbb{Z} : |\bar{k} \text{ (modulo } n)| &= |\bar{k}\bar{1} \text{ (modulo } n)| = |k\bar{1} \text{ (modulo } n)| \\ &= \frac{|\bar{1} \text{ (modulo } n)|}{k \wedge |\bar{1}|} \\ &= \frac{n}{k \wedge n}. \end{aligned}$$

## 2-5 - Groupes monogènes et Groupes cycliques :

### Définition 2-5-1 :

Etant donné un groupe  $G$ .

On dit que  $G$  est un groupe monogène engendré par un élément  $a \in G$  si  $G = \langle a \rangle$ .

Dans ce cas on dit aussi que  $G$  est un groupe monogène.

Si  $G$  est monogène d'ordre fini on dit que  $G$  cyclique.

### Exemples et propriétés 2-5-2 :

- 1)  $\mathbb{Z}$  est un groupe monogène engendré par 1 mais il n'est pas cyclique.
- 2) Soient  $G$  et  $H$  deux groupes et  $f$  un homomorphisme surjectif de  $G$  vers  $H$ .  
Si  $G$  est monogène engendré par un élément  $a$  alors  $H$  est aussi monogène engendré par  $f(a)$ .
- 3) Pour tout entier naturel  $n$ ,  $\mathbb{Z}/n\mathbb{Z}$  est un groupe monogène engendré par  $\bar{1} \text{ (modulo } n)$ .
- 4) Pour tout entier naturel non nul  $n$ ,  $\mathbb{Z}/n\mathbb{Z}$  est un groupe cyclique d'ordre  $n$  engendré par  $\bar{1} \text{ (modulo } n)$ .
- 5)  $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$  est un groupe monogène qui n'est pas cyclique.
- 6) Pour tout entier naturel non nul  $n$ , les groupes cycliques d'ordre  $n$  sont les groupes isomorphes à  $\mathbb{Z}/n\mathbb{Z}$ .  
C'est à dire, si  $n \in \mathbb{N}^*$  et si  $G$  est un groupe alors :  
 $[G \text{ est cyclique d'ordre } n] \Leftrightarrow G \simeq \mathbb{Z}/n\mathbb{Z}$ .
- 7) Les groupes monogènes d'ordres infinis sont les groupes isomorphes à  $\mathbb{Z}$ .  
C'est à dire, pour tout groupe  $G$  on a :  $[G \text{ est monogène infini}] \Leftrightarrow G \simeq \mathbb{Z}$ .
- 8) Tous les sous groupes de  $\mathbb{Z}$  sont monogènes.

### Démonstration :

- 1) Puisque  $\mathbb{Z} = \langle 1 \rangle$  alors  $\mathbb{Z}$  est un groupe monogène engendré par 1.  
Mais  $\mathbb{Z}$  n'est pas cyclique (car  $\mathbb{Z}$  est d'ordre infini).

- 2) Supposons que  $G$  est monogène engendré par un élément  $a$ .  
 $H = f(G) = f(\langle a \rangle) = \langle f(a) \rangle$ .  
Donc  $H$  est aussi monogène engendré par  $f(a)$ .
- 3) Soient  $n$  un entier naturel quelconque et  $p$  la surjection canonique de  $\mathbb{Z}$  vers  $\mathbb{Z}/n\mathbb{Z}$ .  
Puisque  $\mathbb{Z}$  est monogène engendré par 1 et puisque  $p$  est un homomorphisme surjectif de  $\mathbb{Z}$  vers  $\mathbb{Z}/n\mathbb{Z}$  alors (d'après 2)),  $\mathbb{Z}/n\mathbb{Z}$  est un groupe monogène engendré par  $p(1) = \bar{1}$  (modulo  $n$ ).
- 4) Soit  $n$  un entier naturel non nul quelconque.  
Puisque (d'après 3))  $\mathbb{Z}/n\mathbb{Z}$  est monogène et puisque  $\mathbb{Z}/n\mathbb{Z}$  est d'ordre fini  $n$  alors  $\mathbb{Z}/n\mathbb{Z}$  est un groupe cyclique d'ordre  $n$  engendré par  $\bar{1}$  (modulo  $n$ ).
- 5)  $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \simeq \mathbb{Z}$  est un groupe monogène qui n'est pas cyclique.
- 6) Soient  $n$  un entier naturel non nul et  $G$  un groupe.
- ⇒ ) **Si  $G$  est cyclique d'ordre  $n$  :**  
La loi de  $G$  est notée multiplicative.  
Soient  $a$  un générateur de  $G$  et  $f$  l'homomorphisme de  $\mathbb{Z}$  vers  $G$  définie par :  

$$f : \mathbb{Z} \rightarrow G = \langle a \rangle$$

$$k \mapsto f(k) = a^k.$$
Puisque  $G = \langle a \rangle$  est d'ordre fini  $n$ , alors  $a$  est d'ordre fini  $n$ .  
 $|a| = n \Rightarrow G = \langle a \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ .
- ⇐ ) **Si  $G$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$  :**  
Alors il existe un isomorphisme  $f$  de  $\mathbb{Z}/n\mathbb{Z}$  vers  $G$ .  
 $G = f(\mathbb{Z}/n\mathbb{Z}) = f(\langle \bar{1}(\text{modulo } n) \rangle) = \langle f(\bar{1}(\text{modulo } n)) \rangle$ .  
Donc  $G$  est monogène.  
Puisque  $\mathbb{Z}/n\mathbb{Z}$  est d'ordre fini  $n$  et puisque  $G$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$  alors  $G$  est d'ordre fini  $n$ .  
Ce qui montre que  $G$  est cyclique d'ordre  $n$ .
- 7) Soit  $G$ .
- ⇒ ) **Si  $G$  est monogène d'ordre infini :**  
La loi de  $G$  est notée multiplicative.  
Soient  $a$  un générateur de  $G$  et  $f$  l'homomorphisme de  $\mathbb{Z}$  vers  $G$  définie par :  

$$f : \mathbb{Z} \rightarrow G = \langle a \rangle$$

$$k \mapsto f(k) = a^k.$$
Soit  $n$  l'entier naturel tel que  $\ker f = n\mathbb{Z}$ .  
Puisque  $G = H = n\mathbb{Z} = \langle n \rangle$ . est d'ordre infini, alors  $a$  est d'ordre infini.  
Donc  $n = 0$ .  
Par suite  $\ker f = n\mathbb{Z} = 0\mathbb{Z} = \{0\}$ . Donc  $f$  est injectif.  
 $f(\mathbb{Z}) = f(\langle 1 \rangle) = \langle f(1) \rangle = \langle a \rangle = G$ . Alors  $f$  est surjectif.  
Ce qui prouve que  $f$  est bijectif. Par suite  $f$  est un isomorphisme  $f$  de  $\mathbb{Z}$  vers  $G$ .  
Donc  $G$  est isomorphe à  $\mathbb{Z}$ .
- ⇐ ) **Si  $G$  est isomorphe à  $\mathbb{Z}$  :**  
Alors il existe un isomorphisme  $f$  de  $\mathbb{Z}$  vers  $G$ .  
 $G = f(\mathbb{Z}) = f(\langle 1 \rangle) = \langle f(1) \rangle$ . Donc  $G$  est monogène.  
Puisque  $\mathbb{Z}$  est d'ordre infini et puisque  $G$  est isomorphe à  $\mathbb{Z}$  alors  $G$  est d'ordre infini.  
Ce qui montre que  $G$  n'est pas cyclique.
- 8) Soit  $H$  un sous groupe quelconque de  $\mathbb{Z}$ .  
Il existe alors un entier naturel  $n$  tel que  $H = n\mathbb{Z}$ .  
 $H = n\mathbb{Z} = \langle n \rangle$ . Ce qui montre que  $H$  est monogène.

**Proposition 2-5-3 :**

Soient  $G$  un groupe d'ordre fini  $n$  et  $a$  un élément quelconque de  $G$ .

Pour que  $G$  soit cyclique il faut et il suffit que  $a$  soit d'ordre  $n$ .

C'est à dire :  $G = \langle a \rangle \Leftrightarrow |a| = n$ .

**Démonstration :**

$\Rightarrow$ ) Si  $G$  est cyclique engendré par  $a$  :

Alors  $|a| = |\langle a \rangle| = |G| = n$ .

$\Leftarrow$ ) Si  $a$  est d'ordre  $n$  :

$$\begin{cases} \langle a \rangle \subset G \\ |\langle a \rangle| = |a| = n = |G| \end{cases} \Rightarrow G = \langle a \rangle. \text{ Donc } G \text{ est monogène.}$$

Puisque  $G$  est monogène d'ordre fini, alors  $G$  est cyclique.

**Proposition 2-5-4 :**

Si  $G$  est un groupe cyclique multiplicatif engendré par un élément  $a$  alors les générateurs de  $G$  sont les éléments  $a^k$  tels que  $k \wedge |G| = 1$ .

C'est à dire :  $\forall k \in \mathbb{Z} : [a^k \text{ est un générateur de } G] \Leftrightarrow k \wedge |G| = 1$ .

**Démonstration :**

Soient  $G$  un groupe cyclique multiplicatif engendré par un élément  $a$  et  $b$  un élément quelconque de  $G$ .

$b \in G = \langle a \rangle \Rightarrow \exists k \in \mathbb{Z} \text{ tq : } b = a^k$ .

$$G = \langle b \rangle \Leftrightarrow |b| = |G| = |a| \Leftrightarrow |a^k| = |a| \Leftrightarrow \frac{|a|}{k \wedge |a|} = |a| \Leftrightarrow k \wedge |a| = \frac{|a|}{|a|} = 1.$$

Donc les générateurs de  $G$  sont les éléments  $a^k$  tels que  $k \wedge |G| = k \wedge |a| = 1$ .

**Proposition 2-5-5 :**

Si  $G$  est un groupe cyclique additif engendré par un élément  $a$  alors les générateurs de  $G$  sont les éléments  $ka$  tels que  $k \wedge |G| = 1$ .

C'est à dire :  $\forall k \in \mathbb{Z} : [ka \text{ est un générateur de } G] \Leftrightarrow k \wedge |G| = 1$ .

**Démonstration :**

Soient  $G$  un groupe cyclique multiplicatif engendré par un élément  $a$  et  $b$  un élément quelconque de  $G$ .

$b \in G = \langle a \rangle \Rightarrow \exists k \in \mathbb{Z} \text{ tq : } b = ka$ .

$$G = \langle b \rangle \Leftrightarrow |b| = |G| = |a| \Leftrightarrow |ka| = |a| \Leftrightarrow \frac{|a|}{k \wedge |a|} = |a| \Leftrightarrow k \wedge |a| = \frac{|a|}{|a|} = 1.$$

Donc les générateurs de  $G$  sont les éléments  $ka$  tels que  $k \wedge |G| = k \wedge |a| = 1$ .

**Exemple 2-5-6 :**

Pour tout entier naturel non nul  $n$ , les générateurs du groupe cyclique  $\mathbb{Z}/n\mathbb{Z}$  sont les classes  $\bar{k}$  (modulo  $n$ ) tels que  $k \in \mathbb{Z}$  et  $k \wedge n = 1$ .

**Démonstration :**

Soient  $n$  un entier naturel non nul et  $x$  un élément quelconque de  $\mathbb{Z}/n\mathbb{Z}$ .

$x \in \mathbb{Z}/n\mathbb{Z} \Rightarrow \exists k \in \mathbb{Z} \text{ tq : } x = \bar{k} \text{ (modulo } n) = k[\bar{1} \text{ (modulo } n)]$ .

Puisque  $\bar{1}$  (modulo  $n$ ) est un générateur de  $\mathbb{Z}/n\mathbb{Z}$  alors :

$x = \bar{k}$  (modulo  $n$ ) =  $k[\bar{1} \text{ (modulo } n)]$  est un générateur de  $\mathbb{Z}/n\mathbb{Z}$  si seulement si  $k \wedge n = k \wedge |\mathbb{Z}/n\mathbb{Z}| = 1$ .

### **Théorème 2-5-7 :**

Si  $G$  est un groupe monogène alors tous les sous groupes de  $G$  sont monogènes.

### **Démonstration :**

Supposons que  $G$  est un groupe monogène. La loi de  $G$  est notée multiplicative.

Soient  $a$  un générateur de  $G$  et  $f$  l'homomorphisme de  $\mathbb{Z}$  vers  $G$  définie par :

$$\begin{aligned} f : \mathbb{Z} &\rightarrow G = \langle a \rangle \\ k &\mapsto f(k) = a^k. \end{aligned}$$

Soit  $H$  un sous groupe quelconque de  $G$ .

$f^{-1}(H)$  est un sous groupe de  $\mathbb{Z}$ . Donc  $f^{-1}(H)$  est un groupe monogène.

Puisque  $f$  est un homomorphisme surjectif alors  $H = f(f^{-1}(H))$  est monogène.

### **Corollaire 2-5-8 :**

Si  $G$  est un groupe cyclique alors tous les sous groupes de  $G$  sont cycliques.

### **En effet :**

Supposons que  $G$  est un groupe cyclique.

D'après le théorème 2-5-7 tous les sous-groupes de  $G$  sont monogènes qui sont finis.

Donc tous les sous-groupes de  $G$  sont cycliques.

### **Théorème 2-5-9 :**

Si  $G$  est un groupe cyclique d'ordre  $n$  alors pour tout diviseur  $m$  de  $n$  il existe un sous-groupe de  $G$  et un seul d'ordre  $m$ .

### **Démonstration :**

Soient  $G$  un groupe cyclique d'ordre  $n$ ,  $a$  un générateur de  $G$  et  $m$  un diviseur quelconque de  $n$ .

La loi de  $G$  est noté multiplicativement.

- **Existence :**

$$\left| a^{\frac{n}{m}} \right| = \frac{|a|}{\frac{n}{m} \wedge |a|} = \frac{n}{\frac{n}{m} \wedge n} = \frac{n}{\frac{n}{m}} = n \frac{m}{n} = m.$$

Donc  $\langle a^{\frac{n}{m}} \rangle$  est un sous-groupe de  $G$  d'ordre  $m$ .

D'où l'existence d'un sous-groupe de  $G$  d'ordre  $m$ .

- **Unicité :**

Soit  $H$  un sous-groupe quelconque de  $G$  d'ordre  $m$ .

D'après le corollaire 2-5-8,  $H$  est cyclique. Donc il existe un élément  $b$  de  $G$  tel que  $H = \langle b \rangle$ .

$$b \in G = \langle a \rangle \Rightarrow \exists k \in \mathbb{Z}. tq : b = a^k.$$

$$\frac{n}{k \wedge n} = \frac{|a|}{k \wedge |a|} = |a^k| = |b| = |H| = m \Rightarrow k \wedge n = \frac{n}{m} \Rightarrow \frac{n}{m} \mid k \Rightarrow \exists r \in \mathbb{Z}. tq : k = \frac{n}{m}r.$$

$$\text{Alors : } b = a^k = a^{\frac{n}{m}r} = \left(a^{\frac{n}{m}}\right)^r \in \left\langle a^{\frac{n}{m}} \right\rangle \Rightarrow H = \langle b \rangle \subset \left\langle a^{\frac{n}{m}} \right\rangle.$$

$$\begin{cases} H \subset \left\langle a^{\frac{n}{m}} \right\rangle \\ |H| = \left| \left\langle a^{\frac{n}{m}} \right\rangle \right| = n \end{cases} \Rightarrow H = \left\langle a^{\frac{n}{m}} \right\rangle.$$

D'où l'unicité du sous-groupe de  $G$  d'ordre  $m$ .

### 3 - Groupes symétriques :

#### 3-1-Généralités :

**Définition et notation 3-1-1 :**

Soit  $E$  un ensemble.

- ★ L'ensemble des permutations de  $E$  (c'est à dire l'ensemble des bijections de  $E$  vers  $E$ ) est noté  $S(E)$ .
- ★ L'identité de  $E$  est noté  $e_E$  ou  $e$  (c'est à dire  $id_E = e_E$  ou  $id_E = e$ ).
- ★ La loi de composition interne  $\circ$  est notée multiplicativement. C'est à dire :  
 $\forall \sigma, \tau \in S(E) : \sigma \circ \tau$  est noté  $\sigma \tau$ .
- ★ Pour toute permutation  $\sigma \in S(E)$ , on appelle support de  $\sigma$  l'ensemble noté  $supp(\sigma)$  défini par :  $supp(\sigma) = \{x \in E \quad tq : \sigma(x) \neq x\}$ .
- ★ Si  $n$  est un entier naturel non nul et  $E = \{1, 2, \dots, n\}$  alors  $e_E$  est noté  $e_n$  ou  $e$ .
- ★ Si  $n$  est un entier naturel non nul et si  $E = \{1, 2, \dots, n\}$  alors  $S(E)$  est noté aussi  $S_n$ .
- ★ Soient  $n$  est un entier naturel non nul et  $\sigma$  un élément de  $S_n$ . Si on pose  $\sigma(i) = a_i$   
pour tout  $i = 1, 2, \dots, n$  alors  $\sigma$  est notée :  $\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ .

**Remarque 3-1-2 :**

Soient  $n$  un entier naturel non nul et  $\sigma$  un élément de  $S_n$ . Si  $\sigma$  est croissante alors :  
 $\sigma$  est strictement croissante et  $\sigma^{-1}$  est croissante.

**Démonstration :**

On suppose que  $\sigma$  est croissante.

- ★  $\forall i, j = 1, 2, \dots, n$  tels que :  $i < j$ .  

$$\begin{cases} i < j \Rightarrow i \leq j \Rightarrow \sigma(i) \leq \sigma(j) \text{ (car } \sigma \text{ est croissante)} \\ i < j \Rightarrow i \neq j \Rightarrow \sigma(i) \neq \sigma(j) \text{ (car } \sigma \text{ est bijective)} \end{cases} \Rightarrow \sigma(i) < \sigma(j).$$

Donc  $\sigma$  est strictement croissante.

★ Supposons que  $\sigma^{-1}$  n'est pas croissante.  
 Alors :  $\exists i, j = 1, 2, \dots, n$  tels que :  $i < j$  et  $\sigma^{-1}(i) > \sigma^{-1}(j)$ .  
 Puisque  $\sigma$  est strictement croissante alors :  $\sigma(\sigma^{-1}(i)) > \sigma(\sigma^{-1}(j))$   
 Donc :  $(\sigma\sigma^{-1})(i) > (\sigma\sigma^{-1})(j) \Rightarrow e_n(i) > e_n(j) \Rightarrow i > j$  ce qui est absurde.  
 Ce qui montre que  $\sigma^{-1}$  est croissante.

### Proposition 3-1-3 :

Soient  $n$  un entier naturel non nul et  $\sigma$  un élément de  $S_n$ .

Les quatres propriétés suivantes sont équivalentes :

- i)  $\sigma = e_n$ .
- ii)  $\sigma$  est croissante.
- iii)  $\forall i = 1, 2, \dots, n : i \leq \sigma(i)$
- iv)  $\forall i = 1, 2, \dots, n : \sigma(i) \leq i$

### Démonstration :

Montrons : i)  $\Rightarrow$  ii).

Supposons que  $\sigma = e_n$ .

$\forall i, j = 1, 2, \dots, n$  tels que :  $i \leq j : \sigma(i) = e_n(i) = i \leq j = e_n(j) = \sigma(j)$ .

Donc  $\sigma$  est croissante, ce qui montre que ii) est vraie.

Montrons : ii)  $\Rightarrow$  iii)

Supposons que  $\sigma$  est croissante.

Posons  $I = \{i = 1, 2, \dots, n \text{ tq : } i > \sigma(i)\}$  et supposons que  $I$  est non vide.

Soit  $k$  le plus petit élément de  $I$ .

$k \in I \Rightarrow \sigma(k) < k \Rightarrow \sigma(k) \notin I$  (car  $k$  le plus petit élément de  $I$ )  $\Rightarrow \sigma(k) \leq \sigma(\sigma(k))$ .

Puisque  $\sigma$  est croissante alors  $\sigma^{-1}$  est croissante. Par suite on a :

$$\begin{aligned} \sigma^{-1}(\sigma(k)) \leq \sigma^{-1}(\sigma(\sigma(k))) &\Rightarrow (\sigma^{-1}\sigma)(k) \leq (\sigma^{-1}\sigma)(\sigma(k)) \Rightarrow e_n(k) \leq e_n(\sigma(k)) \\ &\Rightarrow k \leq \sigma(k) \Rightarrow k \notin I \text{ ce qui est absurde.} \end{aligned}$$

Alors  $I = \emptyset$ . Donc :  $\forall i = 1, 2, \dots, n : i \leq \sigma(i)$ , ce qui montre que iii) est vraie.

Montrons : iii)  $\Rightarrow$  i)

Supposons que :  $\forall i = 1, 2, \dots, n : i \leq \sigma(i)$

Posons  $I = \{i = 1, 2, \dots, n \text{ tq : } \sigma(i) \neq i\}$  et supposons que  $I$  est non vide.

Soit  $k$  le plus grand élément de  $I$ .

$k \in I \Rightarrow \sigma(k) \neq k \Rightarrow k < \sigma(k) \Rightarrow \sigma(k) \notin I$  (car  $k$  le plus grand élément de  $I$ )

Alors :  $\sigma(\sigma(k)) = \sigma(k) \Rightarrow \sigma(k) = k \Rightarrow k \notin I$ , ce qui est absurde.

Alors  $I = \emptyset$ . Donc :  $\forall i = 1, 2, \dots, n : \sigma(i) = i$ . (c'est à dire que  $\sigma = e_n$ ).

Ce qui montre que i) est vraie.

On a donc montrer que les trois propriétés i), ii) et iii) sont équivalentes.

Montrons : i)  $\Rightarrow$  iv).

Supposons que  $\sigma = e_n$ .

$\forall i = 1, 2, \dots, n : \sigma(i) = e_n(i) = i \leq i$  Donc iv) est vraie.

Montrons : iv)  $\Rightarrow$  i).

Supposons que :  $\forall i = 1, 2, \dots, n : \sigma(i) \leq i$

Posons  $I = \{i = 1, 2, \dots, n \text{ tq : } \sigma(i) \neq i\}$  et supposons que  $I$  est non vide.

Soit  $k$  le plus petit élément de  $I$ .

$k \in I \Rightarrow \sigma(k) \neq k \Rightarrow \sigma(k) < k \Rightarrow \sigma(k) \notin I$  (car  $k$  le plus petit élément de  $I$ )

Alors :  $\sigma(\sigma(k)) = \sigma(k) \Rightarrow \sigma(k) = k \Rightarrow k \notin I$ , ce qui est absurde.

Alors  $I = \emptyset$ . Donc :  $\forall i = 1, 2, \dots, n : \sigma(i) = i$ . (c'est à dire que  $\sigma = e_n$ ).

Ce qui montre que i) est vraie.

Alors i)  $\Leftrightarrow$  iv).

Ce qui montre que es quatres propriétés i), ii), iii) et iv) sont équivalentes.

### Exemples et propriétés 3-1-4 :

Soit  $E$  un ensemble.

- 1)  $e_E$  est l'élément neutre de  $(S(E), \cdot)$   
En particulier si  $n \in \mathbb{N}^*$  et si  $E = \{1, 2, \dots, n\}$  alors  $e_n$  est l'élément neutre de  $(S_n, \cdot)$ .
- 2) Pour tout élément  $\sigma \in S(E)$ , la réciproque  $\sigma^{-1}$  de  $\sigma$  est l'inverse de  $\sigma$ .
- 3)  $(S(E), \cdot)$  est un groupe multiplicatif appelé le groupe symétrique associé à  $E$ .  
En particulier si  $n$  est un entier naturel non nul et si  $E = \{1, 2, \dots, n\}$  alors  $(S_n, \cdot)$  est un groupe multiplicatif appelé le groupe symétrique de degré  $n$ .
- 4)  $S(E)$  est d'ordre fini si et seulement si  $E$  est un ensemble fini, et dans ce cas si  $|E| = n$  alors  $|S(E)| = n!$ .
- 5) Pour tout entier naturel non nul  $n$ , le groupe  $S_n$  est d'ordre  $n!$ . C'est à dire :  
 $\forall n \in \mathbb{N}^* : |S_n| = n!$ .
- 6) Si  $E = \emptyset$  alors  $S(E) = S(\emptyset) = \{\emptyset\} = \{e_\emptyset\}$  est d'ordre  $0! = 1$  et par suite  $S(\emptyset)$  est un groupe abélien.
- 7) Si  $E$  est un singleton (c'est à dire si  $E$  est fini et si  $|E| = 1$ ) alors  $S(E) = \{e_E\}$  est d'ordre  $1! = 1$  et dans ce cas  $S(E)$  est un groupe abélien.  
En particulier  $S_1$  est un groupe abélien.
- 8) Si  $E$  est une paire (c'est à dire si  $E$  est fini et si  $|E| = 2$ ) alors  $S(E)$  est d'ordre  $2! = 2$  et dans ce cas  $S(E)$  est un groupe abélien.  
En particulier  $S_2$  est un groupe abélien.
- 9) Si  $E$  contient au moins trois éléments distincts deux à deux alors  $S(E)$  n'est pas abélien.  
En particulier :  $\forall n \in \mathbb{N}^* : n \geq 3 \Rightarrow S_n$  n'est pas abélien.

#### Démonstrations :

Si  $E$  contient au moins trois éléments  $a, b$  et  $c$  distincts deux à deux.

Soient  $\sigma, \tau \in S(E)$  définies par :

$$\begin{cases} \sigma(a) = b, & \sigma(b) = c, & \sigma(c) = a & \text{et} & \sigma(x) = x : \forall x \in E - \{a, b, c\} \\ \tau(a) = b, & \tau(b) = a & & \text{et} & \tau(x) = x : \forall x \in E - \{a, b\} \end{cases}$$

$$\text{Alors : } \begin{cases} (\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(b) = c \\ (\tau\sigma)(a) = \tau(\sigma(a)) = \tau(b) = a \end{cases} \Rightarrow (\sigma\tau)(a) \neq (\tau\sigma)(a) \Rightarrow \sigma\tau \neq \tau\sigma.$$

Ce qui montre que  $S(E)$  n'est pas abélien.

10)  $\text{supp}(e_E) = \emptyset$ .

11) Soient  $\sigma \in S(E)$ .

a)  $\text{supp}(\sigma) = \emptyset \Leftrightarrow \sigma = e_E$ .

b)  $\sigma(\text{supp}(\sigma)) \subset \text{supp}(\sigma)$  (c'est à dire :  $\forall i \in \text{supp}(\sigma) : \sigma(i) \in \text{supp}(\sigma)$ ).

**En effet :**  $\forall i \in \text{supp}(\sigma) : \sigma(i) \neq i \Rightarrow \sigma(\sigma(i)) \neq \sigma(i) \Rightarrow \sigma(i) \in \text{supp}(\sigma)$ .

Donc :  $\sigma(\text{supp}(\sigma)) \subset \text{supp}(\sigma)$ .

c) Si  $\sigma \neq e_E$  alors  $\text{supp}(\sigma)$  contient au moins deux éléments distincts.

**En effet :**

Puisque  $\sigma \neq e_E$  alors  $\text{supp}(\sigma) \neq \emptyset$ . Donc  $\text{supp}(\sigma)$  contient au moins un élément  $k$ .  
 $k \in \text{supp}(\sigma) \Rightarrow [\sigma(k) \neq k \quad \text{et} \quad k, \sigma(k) \in \text{supp}(\sigma)]$ .

Ce qui montre que  $\text{supp}(\sigma)$  contient au moins les deux éléments  $k$  et  $\sigma(k)$  qui sont distincts.

d)  $\text{supp}(\sigma) = \text{supp}(\sigma^{-1})$ .

**En effet :**

$\subset$ )  $\forall i \in \text{supp}(\sigma) : \sigma(i) \neq i \Rightarrow \sigma^{-1}(\sigma(i)) \neq \sigma^{-1}(i) \Rightarrow i \neq \sigma^{-1}(i) \Rightarrow i \in \text{supp}(\sigma^{-1})$ .

Donc  $\text{supp}(\sigma) \subset \text{supp}(\sigma^{-1})$ .

$\supset$ )  $\forall i \in \text{supp}(\sigma^{-1}) : \sigma^{-1}(i) \neq i \Rightarrow \sigma(\sigma^{-1}(i)) \neq \sigma(i) \Rightarrow i \neq \sigma(i) \Rightarrow i \in \text{supp}(\sigma)$ .

Donc  $\text{supp}(\sigma^{-1}) \subset \text{supp}(\sigma)$ .

Ce qui montre que  $\text{supp}(\sigma) = \text{supp}(\sigma^{-1})$ .

12)  $\forall \sigma, \tau \in S(E) : \text{supp}(\sigma\tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau)$ .

**En effet :**

Supposons  $\text{supp}(\sigma\tau)$  n'est pas inclus dans  $\text{supp}(\sigma) \cup \text{supp}(\tau)$ .

Alors il existe élément  $k \in \text{supp}(\sigma\tau)$  tel que  $k \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$ .

$$k \notin \text{supp}(\sigma) \cup \text{supp}(\tau) \Rightarrow \begin{cases} k \notin \text{supp}(\sigma) \\ k \notin \text{supp}(\tau) \end{cases} \Rightarrow \sigma(k) = \tau(k) = k.$$

$(\sigma\tau)(k) = \sigma(\tau(k)) = \sigma(k) = k \Rightarrow k \in \text{supp}(\sigma\tau)$ . Ce qui est absurde.

Ce qui montre que  $\text{supp}(\sigma\tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau)$ .

13) Soient  $\sigma \in S(E)$ .

a)  $\forall k \in \mathbb{N} : \text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ .

**En effet :**

Montrons par récurrence sur  $k \in \mathbb{N}$  que.

- **Pour  $k = 0$  :**

$$\text{supp}(\sigma^k) = \text{supp}(\sigma^0) = \text{supp}(e_E) = \emptyset \subset \text{supp}(\sigma).$$

- **Pour  $k - 1$  :**

Supposons que  $\text{supp}(\sigma^{k-1}) \subset \text{supp}(\sigma)$ .

- **Pour  $k$  :**

Montrons qu'alors :  $\text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ .

$$\text{supp}(\sigma^{k-1}\sigma) \subset \text{supp}(\sigma^{k-1}) \cup \text{supp}(\sigma) \subset \text{supp}(\sigma) \cup \text{supp}(\sigma) = \text{supp}(\sigma).$$

Ce qui montre que :  $\forall k \in \mathbb{N} : \text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ .

b)  $\forall k \in \mathbb{Z} : \text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ .

**En effet :**

- **Si  $k \geq 0$  :**

Alors :  $k \in \mathbb{N} \Rightarrow \text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ .

- **Si  $k \leq 0$  :**

Alors :  $-k \leq 0 \Rightarrow \text{supp}(\sigma^{-k}) \subset \text{supp}(\sigma^{-1}) = \text{supp}(\sigma)$ .

$$\text{Donc : } \text{supp}(\sigma^k) = \text{supp}((\sigma^k)^{-1}) = \text{supp}(\sigma^{-k}) \subset \text{supp}(\sigma).$$

Ce qui montre que :  $\forall k \in \mathbb{Z} : \text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ .

c)  $\forall u \in \langle \sigma \rangle : \text{supp}(u) \subset \text{supp}(\sigma)$ .

**En effet :**

$\forall u \in \langle \sigma \rangle : \exists k \in \mathbb{Z} \text{ tq : } u = \sigma^k$ . Alors :  $\text{supp}(u) = \text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ .

14) Soient  $\sigma, \tau \in S(E)$ .

Si  $\text{supp}(\sigma)$  et  $\text{supp}(\tau)$  sont disjoints (c'est à dire si  $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$ ) alors les quatres propriétés suivantes sont vérifiers :

i)  $\text{supp}(\sigma\tau) = \text{supp}(\sigma) \cup \text{supp}(\tau)$ .

ii)  $\sigma\tau = \tau\sigma$ .

iii)  $\langle \sigma \rangle \cap \langle \tau \rangle = \{e_E\}$ .

iv) Si de plus  $\sigma$  et  $\tau$  sont d'ordres finis (en particulier si de plus  $E$  est fini) alors  $\sigma\tau$  est d'ordre fini et  $|\sigma\tau| = |\sigma| \vee |\tau|$ .



**Démonstration :**

i) On a montrer dans le cas général que  $\text{supp}(\sigma\tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau)$ .

-  $\forall x \in \text{supp}(\sigma) : x \notin \text{supp}(\tau) \Rightarrow \tau(x) = x \Rightarrow (\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x) \neq x \Rightarrow x \in \text{supp}(\sigma\tau)$ .

Alors :  $\text{supp}(\sigma) \subset \text{supp}(\sigma\tau)$ .

-  $\forall x \in \text{supp}(\tau) : \tau(x) \in \text{supp}(\tau) \Rightarrow \tau(x) \notin \text{supp}(\sigma) \Rightarrow (\sigma\tau)(x) = \sigma(\tau(x)) = \tau(x) \neq x \Rightarrow x \in \text{supp}(\sigma\tau)$ .

Alors :  $\text{supp}(\tau) \subset \text{supp}(\sigma\tau)$ .

Donc :  $\text{supp}(\sigma) \cup \text{supp}(\tau) \subset \text{supp}(\sigma\tau)$ .

Ce qui montre que  $\text{supp}(\sigma\tau) = \text{supp}(\sigma) \cup \text{supp}(\tau)$ .

ii)  $\forall x \in E :$

- **Si  $x \in \text{supp}(\sigma)$  :**

Alors  $\sigma(x) \in \text{supp}(\sigma) \Rightarrow x, \sigma(x) \notin \text{supp}(\tau)$ .

Donc :  $(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x) = \tau(\sigma(x)) = (\tau\sigma)(x)$ .

- **Si  $x \in \text{supp}(\tau)$  :**

Alors  $\tau(x) \in \text{supp}(\tau) \Rightarrow x, \tau(x) \notin \text{supp}(\sigma)$ .

Donc :  $(\sigma\tau)(x) = \sigma(\tau(x)) = \tau(x) = \tau(\sigma(x)) = (\tau\sigma)(x)$ .

- **Si  $x \notin \text{supp}(\sigma)$  et si  $x \notin \text{supp}(\tau)$  :**

Alors :  $x \notin \text{supp}(\sigma) \cup \text{supp}(\tau) = \text{supp}(\sigma\tau) = \text{supp}(\tau\sigma)$ .

Donc :  $(\sigma\tau)(x) = x = (\tau\sigma)(x)$ .

Ce qui montre que  $\sigma\tau = \tau\sigma$ .

iii)  $\forall u \in \langle\sigma\rangle \cap \langle\tau\rangle : \text{supp}(u) \subset \text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset \Rightarrow u = e_E$ .

Donc :  $\langle\sigma\rangle \cap \langle\tau\rangle = \{e_E\}$ .

iv) Supposons que  $\sigma$  et  $\tau$  sont d'ordres finis (en particulier si de plus  $E$  est fini).

Puisque  $\sigma, \tau$  sont d'ordres finis,  $\sigma\tau = \tau\sigma$  et  $\langle\sigma\rangle \cap \langle\tau\rangle = \{e_E\}$ .

Alors (d'après les propriétés de II 4))  $\sigma\tau$  est d'ordre fini et  $|\sigma\tau| = |\sigma| \vee |\tau|$ .

15) Soient  $\sigma \in S(E)$  d'ordre fini (en particulier  $E$  est fini),  $a \in E$  et

$I = \{i \in \mathbb{Z} \text{ tq } \sigma^i(a) = a\}$ .

a)  $|\sigma| \in I$  car  $\sigma^{|\sigma|}(a) = e_E(a) = a$ .

b) Il existe un entier naturel non nul  $k$  tel que  $I = k\mathbb{Z}$ .

**Démonstration :**

$|\sigma| \in I \Rightarrow I \neq \emptyset$ .

$\forall i, j \in I : \sigma^{i+j}(a) = (\sigma^i\sigma^j)(a) = \sigma^i(\sigma^j(a)) = \sigma^i(a) = a \Rightarrow i+j \in I$ .

$\forall i \in I : \sigma^{-i}(a) = \sigma^{-i}(\sigma^i(a)) = (\sigma^{-i}\sigma^i)(a) = e_E(a) = a \Rightarrow -i \in I$ .

Donc  $I$  est un sous groupe de  $(\mathbb{Z}, +)$ , par suite il existe un entier naturel  $k$  tel que  $I = k\mathbb{Z}$ .

$[|\sigma| \in I \text{ et } |\sigma| = 0] \Rightarrow I \neq \{0\} = 0\mathbb{Z} \Rightarrow k \neq 0$ .

c)  $k$  vérifie les trois propriétés suivantes :

i)  $\sigma^k(a) = a$ .

ii)  $a, \sigma(a), \dots, \sigma^{k-1}(a)$  sont distincts deux à deux.

iii)  $\{a, \sigma(a), \dots, \sigma^{k-1}(a)\} = \{\tau(a) \text{ tq } \tau \in \langle\sigma\rangle\}$ .

**Démonstration :**

i)  $k \in k\mathbb{Z} = I \Rightarrow \sigma^k(a) = a$ .

ii) Soient  $i, j = 0, 1, \dots, k-1$  tels que :  $i \geq j$  et  $\sigma^i(a) = \sigma^j(a)$ .

$\sigma^i(a) = \sigma^j(a) \Rightarrow \sigma^{-j}(\sigma^i(a)) = \sigma^{-j}(\sigma^j(a)) \Rightarrow (\sigma^{-j}\sigma^i)(a) = (\sigma^{-j}\sigma^j)(a) \Rightarrow \sigma^{-j+i}(a) = (\sigma^{-j+j})(a) \Rightarrow \sigma^{i-j}(a) = e_E(a) = a \Rightarrow i-j \in I = k\mathbb{Z} \Rightarrow \exists l \in \mathbb{Z} \text{ tq } i-j = kl$ .

$$0 \leq i-j \leq i \leq k-1 < k \Rightarrow 0 \leq kl < k \Rightarrow 0 \leq l < 1 \Rightarrow l = 0.$$

$$\text{Donc : } i-j = kl = k0 = 0 \Rightarrow i = j.$$

Ce qui montre que  $a, \sigma(a), \dots, \sigma^{k-1}(a)$  sont distincts deux à deux.

iii) Posons  $A = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$  et  $B = \{\tau(a) \text{ tq : } \tau \in \langle \sigma \rangle\}$ .

$$\subset ) \forall i = 0, 1, \dots, k-1 : \sigma^i \in \langle \sigma \rangle \Rightarrow \sigma^i(a) \in B.$$

$$\text{Donc : } A \subset B.$$

$$\supset ) \forall x \in B : \exists \tau \in \langle \sigma \rangle \text{ tq : } x = \tau(a).$$

Puisque  $\tau \in \langle \sigma \rangle$  alors il existe  $j \in \mathbb{Z}$  tel que  $\tau = \sigma^j$ .

$$j \in \mathbb{Z} \Rightarrow \exists l, i \in \mathbb{Z} \text{ tq : } \begin{cases} j = kl + i \\ 0 \leq i \leq k-1 \end{cases}.$$

$$kl \in k\mathbb{Z} = I \Rightarrow \sigma^{kl}(a) = a.$$

$$\text{Donc : } x = \tau(a) = \sigma^j(a) = \sigma^{kl+i}(a) = (\sigma^i \sigma^{kl})(a) = \sigma^i(\sigma^{kl}(a)) = \sigma^i(a) \in A.$$

$$\text{Par suite } B \subset A.$$

Ce qui montre que :  $\{a, \sigma(a), \dots, \sigma^{k-1}(a)\} = A = B = \{\tau(a) \text{ tq : } \tau \in \langle \sigma \rangle\}$ .

### Exemple 3-1-5 :

Pour  $n = 11$ ,  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 4 & 1 & 5 & 6 & 2 & 3 & 8 & 11 & 10 & 9 \end{pmatrix}$  et  $a = 6$  on a :

$$\sigma(6) = 2, \sigma^2(6) = \sigma(2) = 4, \sigma^3(6) = \sigma(4) = 5 \text{ et } \sigma^4(6) = \sigma(5) = 6.$$

$$\text{Donc : } \begin{cases} k = 4 \text{ et } \sigma^4(6) = 6 \\ 6, \sigma(6) = 2, \sigma^2(6) = 4, \sigma^3(6) = 5 \text{ sont distincts deux à deux} \\ \{6, \sigma(6) = 2, \sigma^2(6) = 4, \sigma^3(6) = 5\} = \{\tau(6) \text{ tq : } \tau \in \langle \sigma \rangle\} \end{cases}$$

## 3-2-Cycles :

### Définition 3-2-1 :

Soient  $E$  un ensemble,  $k$  un entier naturel tel que  $k \geq 2$  et  $a_1, a_2, \dots, a_k$  des éléments de  $E$  distincts deux à deux. On appelle  $k$ -cycle  $a_1, a_2, \dots, a_k$  la permutation notée  $(a_1, a_2, \dots, a_k)$  définie par :

$$(a_1, a_2, \dots, a_k) : E \rightarrow E$$

$$a_i \mapsto a_{i+1} \quad \text{si } 1 \leq i \leq k-1$$

$$a_k \mapsto a_1$$

$$x \mapsto x \quad \text{si } x \notin \{a_1, a_2, \dots, a_k\}.$$

On dit aussi que  $(a_1, a_2, \dots, a_k)$  est un  $k$ -cycle ou un cycle de type  $k$  ou un cycle.

Si  $k = 2$  on dit que  $(a_1, a_2)$  est une transposition.

### Exemple 3-2-2 :

Pour  $n = 7$

$$\star (2, 7, 4, 3) \text{ est un 4-cycle. } (2, 7, 4, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}.$$

$$\star (2, 4) \text{ est une transposition. } (2, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 2 & 5 & 6 & 7 \end{pmatrix}.$$

### Propriétés 3-2-3 :

Soient  $E$  un ensemble et  $\sigma = (a_1, a_2, \dots, a_k)$  un cycle.

- 1)  $\text{supp}(\sigma) = \{a_1, a_2, \dots, a_k\}$ .
- 2)  $\forall i = 1, \dots, k : a_i = \sigma^{i-1}(a_1)$ .
- 3)  $\sigma^k(a_1) = a_1$ .
- 4)  $\sigma^k = e_E$ .
- 5) Le  $k$ -cycle  $\sigma = (a_1, a_2, \dots, a_k)$  est d'ordre  $k$ .
- 6)  $\forall x, y \in \text{supp}(\sigma) : \exists \tau \in \langle \sigma \rangle \text{ tq } : y = \tau(x)$ .
- 7)  $\forall x \in \text{supp}(\sigma) : x, \sigma(x), \dots, \sigma^{k-1}(x)$  sont distincts deux à deux.
- 8)  $\forall x \in \text{supp}(\sigma) : \text{sup}(\sigma) = \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$ .
- 9)  $\forall x \in \text{supp}(\sigma) : \sigma = (x, \sigma(x), \dots, \sigma^{k-1}(x))$ .
- 10) Pour  $k = 2 : \sigma = (a_1, a_2) = (a_2, a_1)$ .
- 11) Si  $k \geq 3$  alors pour tout entier naturel  $r \in \{2, \dots, k-1\}$ ,  
 $\sigma = (a_1, a_2, \dots, a_k) = (a_1, \dots, a_r)(a_r, \dots, a_k)$
- 12)  $\sigma^{-1} = (a_1, a_2, \dots, a_k)^{-1} = (a_k, a_{k-1}, \dots, a_1)$ .

### Démonstration :

- 1) Posons  $A = \{a_1, a_2, \dots, a_k\}$ .
    - $\forall x \in A : \exists i = 1, \dots, k \text{ tq } : x = a_i$ .  
Donc  $A \subset \text{supp}(\sigma)$ .  
$$\begin{cases} \sigma(x) = \sigma(a_i) = a_{i+1} \neq a_i = x & \text{si } i \neq k \\ \sigma(x) = \sigma(a_i) = \sigma(a_k) = a_1 \neq a_k = a_i = x & \text{si } i = k \end{cases} \text{ . Alors } x \in \text{supp}(\sigma).$$
  
Donc  $A \subset \text{supp}(\sigma)$ .
    - $\forall x \in E - A : \sigma(x) = x \Rightarrow x \notin \text{supp}(\sigma)$ .  
Donc  $\text{supp}(\sigma) \subset A$ .  
Ce qui montre que  $\text{supp}(\sigma) = A = \{a_1, a_2, \dots, a_k\}$ .
  - 2) Posons  $I = \{i = 1, \dots, k \text{ tq } : a_i \neq \sigma^{i-1}(a_1)\}$  et supposons que  $I$  est non vide.  
Soit  $j$  le plus petit élément de  $I$ .  
 $a_1 = e_E(a_1) = \sigma^0(a_1) = \sigma^{1-1}(a_1) \Rightarrow 1 \notin I \Rightarrow j \neq 1 \Rightarrow j \geq 2 \Rightarrow j-1 \geq 1$ .  
Puisque  $j-1 \notin I$  (car  $j-1 < j$ ) et puisque  $j-1 \geq 1$  alors :  
 $a_{j-1} = \sigma^{j-1-1}(a_1) = \sigma^{j-2}(a_1)$ .  
Par suite on a :  $a_j = \sigma(a_{j-1}) = \sigma(\sigma^{j-2}(a_1)) = (\sigma\sigma^{j-2})(a_1) = \sigma^{j-1}(a_1) \Rightarrow j \notin I$ .  
Ce qui est absurde. Donc :  $I = \emptyset$ .  
Ce qui montre que :  $\forall i = 1, 2, \dots, k : a_i = \sigma^{i-1}(a_1)$ .
  - 3)  $\sigma^k(a_1) = (\sigma\sigma^{k-1})(a_1) = \sigma(\sigma^{k-1}(a_1)) = \sigma(a_k) = a_1$ .
  - 4) Soit  $x$  un élément quelconque de  $E$ .
    - Si  $x \notin \text{supp}(\sigma)$  :  
Alors :  $x \notin \text{supp}(\sigma^k)$  (car  $\text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ ). Donc :  $\sigma^k(x) = x = e_E(x)$ .
    - Si  $x \in \text{supp}(\sigma)$  :  
 $\exists i = 1, \dots, k \text{ tq } : x = a_i$ .  
Alors :  $\sigma^k(x) = \sigma^k(a_i) = \sigma^k(\sigma^{i-1}(a_1)) = (\sigma^k\sigma^{i-1})(a_1) = (\sigma^{i-1}\sigma^k)(a_1) = \sigma^{i-1}(\sigma^k(a_1))$   
 $= \sigma^{i-1}(a_1) = a_i = x$   
 $= e_E(x)$ .
- Donc  $\sigma^k = e_E$ .

- 5) •  $\forall i = 1, 2, \dots, k-1 : \sigma^i(a_1) = \sigma^{i+1-1}(a_1) = a_{i+1} \neq a_1 = e_E(a_1)$ . Alors :  $\sigma^i \neq e_E$ .  
Donc :  $|\sigma| \geq k$ .  
•  $\sigma^k = e_E \Rightarrow |\sigma|k \Rightarrow |\sigma| \geq k$ .  
Ce qui montre que  $|\sigma| = k$ .
- 6)  $\forall x, y \in \text{supp}(\sigma) : \exists i, j = 1, 2, \dots, k$  tq :  $[x = a_i \text{ et } y = a_j]$ .  
 $x = a_i = \sigma^{i-1}(a_1) \Rightarrow a_1 = \sigma^{1-i}(x)$ .  
Donc :  $y = a_j = \sigma^{j-1}(a_1) = \sigma^{j-1}(\sigma^{1-i}(x)) = (\sigma^{j-1}\sigma^{1-i})(x) = \sigma^{j-i}(x)$ .  
Il suffit de prendre  $\tau = \sigma^{j-i} \in \langle \sigma \rangle$  et on a :  $y = \tau(x)$ .
- 7) Soit  $x$  un élément de  $\text{supp}(\sigma)$  et soient  $i, j = \{1, \dots, k-1\}$  tels que  $i \neq j$ .  
 $x \in \text{supp}(\sigma) \Rightarrow \exists \tau \in \langle \sigma \rangle$  tq :  $x = \tau(a_1)$  (d'après 6)).  
Alors :  $\sigma^i(x) = \sigma^i(\tau(a_1)) = (\sigma^i\tau)(a_1) = (\tau\sigma^i)(a_1) = \tau(\sigma^i(a_1)) = \tau(a_{i+1})$   
 $\neq \tau(a_{j+1}) = \tau(\sigma^j(a_1)) = (\tau\sigma^j)(a_1) = (\sigma^j\tau)(a_1) = \sigma^j(\tau(a_1)) = \sigma^j(x)$ .  
Ce qui montre que :  $\forall x \in \text{supp}(\sigma) : x, \sigma(x), \dots, \sigma^{k-1}(x)$  sont distincts deux à deux.
- 8)  $\subset$  )  $\forall y \in \text{supp}(\sigma) : \exists \tau \in \langle \sigma \rangle$  tq :  $y = \tau(x)$ .  
Puisque  $\sigma$  est d'ordre  $k$  alors il existe  $i = 1, 2, \dots, k-1$  tq :  $\tau = \sigma^i$ .  
Donc  $y = \sigma^i(x) \in A$ .  
Alors :  $\text{supp}(\sigma) \subset A$ .  
 $\supset$  ) Puisque  $x \in \text{supp}(\sigma)$  alors  $x, \sigma(x), \dots, \sigma^{k-1}(x) \in \text{supp}(\sigma)$ .  
Donc :  $A \subset \text{supp}(\sigma)$ .  
Ce qui montre que :  $\text{supp}(\sigma) = A = \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$ .
- 9) Soient  $x$  un élément quelconque de  $\text{supp}(\sigma)$  et  $\tau = (x, \sigma(x), \dots, \sigma^{k-1}(x))$ .  
 $\forall y \in E$  :  
- **Si  $y \notin \text{supp}(\sigma)$  :**  
Alors (d'après 8)) :  $y \notin \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$ . Donc :  $\sigma(y) = y = \tau(y)$ .  
- **Si  $y \in \text{supp}(\sigma)$  :**  
Alors (d'après 8)) :  $y \in \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$ .  
Donc :  $\exists i = 1, 2, \dots, k-1$  tq :  $y = \sigma^i(x)$ . Par suite :  
• **Si  $i \neq k-1$  :**  
 $\sigma(y) = \sigma(\sigma^i(x)) = (\sigma\sigma^i)(x) = \sigma^{i+1}(x) = \tau(\sigma^i(x)) = \tau(y)$ .  
• **Si  $i = k-1$  :**  
 $\sigma(y) = \sigma(\sigma^{k-1}(x)) = (\sigma\sigma^{k-1})(x) = \sigma^{k-1+1}(x) = \sigma^k(x) = x = \tau(\sigma^{k-1}(x)) = \tau(\sigma^i(x))$   
 $= \tau(y)$ .  
Ce qui prouve que :  $\sigma = \tau = (x, \sigma(x), \dots, \sigma^{k-1}(x))$ .
- 10) Pour  $k = 2$  :  
Puisque (d'après 1))  $a_2 \in \text{supp}(\sigma) = \{a_1, a_2\}$  alors (d'après 9)) :  
 $\sigma = (a_1, a_2) = (a_2, \sigma(a_2)) = (a_2, a_1)$ .
- 11) Supposons que  $k \geq 3$  et soit  $r$  un élément quelconque de l'ensemble  $\{2, \dots, k-1\}$ .  
Posons :  $u = (a_1, \dots, a_r)$  et  $v = (a_r, \dots, a_k)$   
 $\forall x \in E$  :  
- **Si  $x \notin \text{supp}(\sigma)$  :**  
Alors :  $(uv)(x) = u(v(x)) = u(x) = x = \sigma(x) \Rightarrow \sigma(x) = (uv)(x)$ .  
- **Si  $x \in \text{supp}(\sigma)$  :**  
Alors :  $\exists i = 1, \dots, k$  tq :  $x = a_i$ .  
• **Si  $i \leq r-1$  :**  
Alors :  $\sigma(x) = \sigma(a_i) = a_{i+1} = u(a_i) = u(v(a_i)) = (uv)(a_i) = (uv)(x)$ .  
• **Si  $r \leq i \leq k-1$  :**  
Alors :  $\sigma(x) = \sigma(a_i) = a_{i+1} = u(a_{i+1}) = u(v(a_i)) = (uv)(a_i) = (uv)(x)$ .

- Si  $i = k$  :

$$\text{Alors : } \sigma(x) = \sigma(a_i) = \sigma(a_k) = a_1 = u(a_r) = u(v(a_k)) = (uv)(a_k) = (uv)(a_i) = (uv)(x).$$

$$\text{Donc : } \sigma = (a_1, a_2, \dots, a_k) = uv = (a_1, \dots, a_r)(a_r, \dots, a_k)$$

12) Posons  $\tau = (a_k, a_{k-1}, \dots, a_1)$ .

$$\forall x \in E :$$

- Si  $x \notin \text{supp}(\sigma)$  :

$$\text{Alors : } (\tau\sigma)(x) = \tau(\sigma(x)) = \tau(x) = x = e_E(x).$$

- Si  $x \in \text{supp}(\sigma)$  :

$$\text{Alors : } \exists i = 1, \dots, k \text{ tq : } x = a_i.$$

- Si  $i \leq k-1$  :

$$\text{Alors : } (\tau\sigma)(x) = \tau(\sigma(x)) = \tau(\sigma(a_i)) = \tau(a_{i+1}) = a_i = x = e_E(x).$$

- Si  $i \leq k$  :

$$\text{Alors : } (\tau\sigma)(x) = \tau(\sigma(x)) = \tau(\sigma(a_i)) = \tau(\sigma(a_k)) = \tau(a_1) = a_k = x = e_E(x).$$

$$\text{Donc : } \tau\sigma = e_E \Rightarrow \sigma^{-1} = (a_1, a_2, \dots, a_k)^{-1} = \tau = (a_k, a_{k-1}, \dots, a_1).$$

### Exemple 3-2-4 :

Pour  $n = 11$ , soit  $\sigma = (2, 11, 4, 7, 3, 8)$ .

- $\text{supp}\sigma = \text{supp}((2, 11, 4, 7, 3, 8)) = \{2, 11, 4, 7, 3, 8\}$ .
- $2 = \sigma^0(2)$ ,  $11 = \sigma^1(2)$ ,  $4 = \sigma^2(2)$ ,  $7 = \sigma^3(2)$ ,  $3 = \sigma^4(2)$  et  $8 = \sigma^5(2)$
- $|\sigma| = 6$ .
- $\sigma = (2, 11, 4, 7, 3, 8) = (11, 4, 7, 3, 8, 2) = (4, 7, 3, 8, 2, 11) = (7, 3, 8, 2, 11, 4) = (3, 8, 2, 11, 4, 7) = (8, 2, 11, 4, 7, 3)$ .
- $\sigma = (2, 11, 4, 7, 3, 8) = (2, 11)(11, 4, 7, 3, 8) = (2, 11, 4)(4, 7, 3, 8) = (2, 11, 4, 7)(7, 3, 8) = (2, 11, 4, 7, 3)(3, 8)$ .
- $\sigma^{-1} = (2, 11, 4, 7, 3, 8)^{-1} = (8, 3, 7, 4, 11, 2)$ .

### Corollaire 3-2-5 :

Soit  $E$  un ensemble. Si  $\sigma = (a_1, \dots, a_k)$  est un cycle alors :

$$\sigma = \prod_{i=1}^{k-1} (a_i, a_{i+1}) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k).$$

### Démonstration :

Montrons par récurrence que pour tout entier naturel  $k \geq 2$  et pour tout  $k$ -cycle

$$\sigma = (a_1, \dots, a_k) \in S(E), \sigma = \prod_{i=1}^{k-1} (a_i, a_{i+1}).$$

- Pour  $k = 2$  :

$$\text{Soit } \sigma = (a_1, \dots, a_k) \in S(E).$$

$$\sigma = (a_1, \dots, a_k) = (a_1, a_2) = \prod_{i=1}^1 (a_i, a_{i+1}) = \prod_{i=1}^{2-1} (a_i, a_{i+1}) = \prod_{i=1}^{k-1} (a_i, a_{i+1}).$$

- Pour  $k-1$  :

Supposons que pour tout  $(k-1)$ -cycle  $\sigma = (a_1, \dots, a_{k-1}) \in S(E)$  on a :

$$\sigma = (a_1, \dots, a_{k-1}) = \prod_{i=1}^{k-2} (a_i, a_{i+1}).$$

- **Pour k :**

Montrons qu'alrs pour tout  $k$ -cycle  $\sigma = (a_1, \dots, a_k) \in S(E)$  on a :

$$\sigma = (a_1, \dots, a_k) = \prod_{i=1}^{k-1} (a_i, a_{i+1}).$$

Soit  $\sigma = (a_1, \dots, a_k)$  un  $k$ -cycle quelconque de  $S(E)$ .

D'après la propriété 11) du théorème 3-2-4,  $\sigma = (a_1, \dots, a_k) = (a_1, \dots, a_{k-1})(a_{k-1}, a_k)$ .

D'après l'hypothèse de récurrence, on a donc :

$$\sigma = (a_1, \dots, a_k) = \prod_{i=1}^{k-2} (a_i, a_{i+1})(a_{k-1}, a_k) = \prod_{i=1}^{k-1} (a_i, a_{i+1}) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k).$$

**Exemple 3-2-6 :**

Pour  $n = 11$ , soit  $\sigma = (2, 11, 4, 7, 3, 8)$ .

$$\sigma = (2, 11, 4, 7, 3, 8) = (2, 11)(11, 4)(4, 7)(7, 3)(3, 8).$$

**Corllaire 3-2-7 :**

Soit  $E$  un ensemble. Un cycle quelconque de  $S(E)$  est un produit de transpositions.

**En effet :**

Soit  $\sigma$  un cycle quelconque de  $S(E)$ .

Il existe alors des éléments  $a_1, \dots, a_k$  de  $E$  distincts deux à deux tels que  $\sigma = (a_1, \dots, a_k)$ .

D'après le corollaire 3-2-5,  $\sigma = \prod_{i=1}^{k-1} (a_i, a_{i+1}) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$ .

Donc  $\sigma$  est le produit des transpositions  $(a_1, a_2), (a_2, a_3), \dots, (a_{k-1}, a_k)$ .

**Lemme 3-2-8 :**

Soient  $E$  un ensemble,  $\sigma \in S(E)$  d'ordre fini (en particulier  $E$  est un ensemble fini). et  $a$  un élément quelconque de  $\text{sup } \sigma$ .

Il existe un entier naturel non nul  $k$  et un seul tel que :

$$\begin{cases} a, \sigma(a), \dots, \sigma^{k-1}(a) \text{ sont distincts deux à deux} \\ \sigma^k(a) = a \end{cases}.$$

**Démonstration :**

- **Existence :**

Soit  $I = \{i \in \mathbb{N}^* \text{ tq : } \sigma^i(a) = a\}$ .

$\sigma^{|\sigma|}(a) = e_E(a) = a \Rightarrow |\sigma| \in I \Rightarrow I \neq \emptyset$ . Soit  $k$  le plus petit élément de  $I$ .

•  $k \in I \Rightarrow \sigma^k(a) = a$ .

• Supposons qu'il existe deux éléments  $i$  et  $j$  de  $\{0, 1, \dots, k-1\}$  tels que  $i > j$  et  $\sigma^i(a) = \sigma^j(a)$ .

Alors :  $\sigma^{-j}(\sigma^i(a)) = \sigma^{-j}(\sigma^j(a)) \Rightarrow (\sigma^{-j}\sigma^i)(a) = (\sigma^{-j}\sigma^j)(a) \Rightarrow \sigma^{i-j}(a) = e_E(a) = a$ .

Donc :  $i-j \in I$  (car  $i-j \in \mathbb{N}^*$  et  $\sigma^{i-j}(a) = a$ )  $\Rightarrow i-j \geq k$ .

Par suite :  $k \leq i-j \leq i \leq k-1 < k$ . Ce qui est absurde.

Ce qui montre que  $a = \sigma^0(a) = e_E(a), \sigma(a), \dots, \sigma^{k-1}(a)$  sont distincts deux à deux.

- **Uncité :**

Soit  $h$  un entier naturel non nul quelconque tel que :

$$\begin{cases} a, \sigma(a), \dots, \sigma^{h-1}(a) \text{ sont distincts deux à deux} \\ \sigma^h(a) = a \end{cases}.$$

$$[h \in \mathbb{N}^* \text{ et } \sigma^h(a) = a] \Rightarrow h \in I \Rightarrow h \geq k.$$

Supposons que  $h > k$ . Alors :  $k \in \{1, \dots, h-1\} \Rightarrow a \neq \sigma^k(a) = a$ .

Ce qui est absurde. Donc  $h = k$ .

D'où l'unicité de l'entier naturel  $k$  tel que :

$$\begin{cases} a, \sigma(a), \dots, \sigma^{k-1}(a) \text{ sont distincts deux à deux} \\ \sigma^k(a) = a \end{cases}.$$

**Théorème 3-2-9 :**

Soient  $E$  un ensemble,  $\sigma \in S(E)$  d'ordre fini (en particulier  $E$  est un ensemble fini). et  $a$  un élément quelconque de  $\text{supp } \sigma$ .

Pour que  $\sigma$  soit un cycle il faut et il suffit que :  $\forall x \in \text{supp}(\sigma) : \exists \tau \in \langle \sigma \rangle \text{ tq : } x = \tau(a)$ .

**Démonstration :**

$\Rightarrow$  ) **Si  $\sigma$  est un cycle :**

Alors (d'après la propriété 2-3-3-6)) :  $\forall x \in \text{supp}(\sigma) : \exists \tau \in \langle \sigma \rangle \text{ tq : } x = \tau(a)$ .

$\Leftarrow$  ) **Si on a :**  $\forall x \in \text{supp}(\sigma) : \exists \tau \in \langle \sigma \rangle \text{ tq : } x = \tau(a)$  :

D'après le lemme 3-2-8, il existe un entier naturel non nul  $k$  tel que :

$$\begin{cases} a, \sigma(a), \dots, \sigma^{k-1}(a) \text{ sont distincts deux à deux} \\ \sigma^k(a) = a \end{cases}.$$

• Montrons que  $\text{supp}(\sigma) = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$ .

$\subset$  )  $\forall x \in \text{supp}(\sigma) : \exists \tau \in \langle \sigma \rangle \text{ tq : } x = \tau(a)$ .

$$\tau \in \langle \sigma \rangle \Rightarrow \exists j \in \mathbb{Z}^* \text{ tq : } \tau = \sigma^j. \exists q, i \in \mathbb{Z} \text{ tq : } \begin{cases} j = kq + i \\ 0 \leq i \leq k-1 \end{cases}.$$

$$\sigma^k(a) = a \Rightarrow a \notin \text{supp} \sigma^k$$

$$\Rightarrow a \notin (\text{supp} \sigma^k)^q = \text{supp} \sigma^{kq} \text{ (car } (\text{supp} \sigma^k)^q \subset \text{supp} \sigma^k)$$

$$\Rightarrow \sigma^{kq}(a) = a.$$

$$\text{Donc : } x = \tau(a) = \sigma^j(a) = \sigma^{kq+i}(a) = \sigma^{i+kq}(a) = (\sigma^i \sigma^{kq})(a) = \sigma^i(\sigma^{kq}(a)) \\ = \sigma^i(a) \in \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}.$$

Par suite  $\text{supp} \sigma \subset \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$ .

$\supset$  )  $\forall x \in \{a, \sigma(a), \dots, \sigma^{k-1}(a)\} : \exists i = 0, \dots, k-1 \text{ tq : } x = \sigma^i(a)$ .

- **Si  $i \neq k-1$  :**

$$\sigma(x) = \sigma(\sigma^i(a)) = (\sigma \sigma^i)(a) = \sigma^{i+1}(a) \neq \sigma^i(a) = x \Rightarrow x \in \text{supp} \sigma.$$

- **Si  $i = k-1$  :**

$$\sigma(x) = \sigma(\sigma^{k-1}(a)) = (\sigma \sigma^{k-1})(a) = \sigma^k(a) = a \neq \sigma^{k-1}(a) = x \Rightarrow x \in \text{supp} \sigma.$$

Par suite  $\{a, \sigma(a), \dots, \sigma^{k-1}(a)\} \subset \text{supp} \sigma$ .

Oon a alors :  $\text{supp} \sigma = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$ .

- Montrons que  $\sigma = (a, \sigma(a), \dots, \sigma^{k-1}(a))$ .

Posons  $\tau = (a, \sigma(a), \dots, \sigma^{k-1}(a))$ .

$\forall x \in E$  :

- Si  $x \notin \text{supp}(\sigma) = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$  :

$$\sigma(x) = x = \tau(x).$$

- Si  $x \in \text{supp}(\sigma) = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$  :

$$\exists i = 0, 1, \dots, k-1 \text{ tq : } x = \sigma^i(a).$$

★ Si  $i \neq k-1$  :

$$\sigma(x) = \sigma(\sigma^i(a)) = (\sigma\sigma^i)(a) = \sigma^{i+1}(a) = \tau(\sigma^i(a)) = \tau(x).$$

★ Si  $i = k-1$  :

$$\sigma(x) = \sigma(\sigma^{k-1}(a)) = (\sigma\sigma^{k-1})(a) = \sigma^k(a) = a = \tau(\sigma^{k-1}(a)) = \tau(x).$$

Par suite  $\sigma = \tau = (a, \sigma(a), \dots, \sigma^{k-1}(a))$ .

Ce qui montre que  $\sigma$  est un cycle.

### Corollaire 3-2-10 :

Soient  $E$  un ensemble fini et  $\sigma \in S(E)$ .

Pour que  $\sigma$  soit un cycle il faut et il suffit que :

$$\begin{cases} \text{supp}\sigma \neq \emptyset \\ \forall x, y \in \text{supp}\sigma : \exists \tau \in \langle \sigma \rangle \text{ tq : } y = \tau(x) \end{cases}.$$

### Démonstration :

$\Rightarrow$  ) Si  $\sigma$  est un cycle :

Alors (d'après la propriété 2-3-3-6)) :

$$\begin{cases} \text{supp}\sigma \neq \emptyset \\ \forall x, y \in \text{supp}\sigma : \exists \tau \in \langle \sigma \rangle \text{ tq : } y = \tau(x) \end{cases}.$$

$\Leftarrow$  ) Si  $\text{supp}(\sigma) \neq \emptyset$  et si on a :  $\forall x, y \in \text{supp}\sigma : \exists \tau \in \langle \sigma \rangle \text{ tq : } y = \tau(x)$  :

Puisque  $\text{supp}\sigma \neq \emptyset$ , il existe un élément  $a \in \text{supp}\sigma$ .

Par suite on a :  $\forall x \in \text{supp}\sigma : \exists \tau \in \langle \sigma \rangle \text{ tq : } x = \tau(a)$ .

D'après le théorème 3-2-9,  $\sigma$  est un cycle.

### 3-3-Décomposition d'une permutation :

#### Définition et notation 3-3-1 :

Soient  $E$  un ensemble,  $\sigma$  une permutation de  $E$  et  $A$  une partie de  $E$ . on dit que  $A$  est une partie stable de  $E$  par  $\sigma$  si on a  $\sigma(A) = A$ , et dans ce cas on note par  $\sigma_A$

l'application suivante :  $\sigma_A : E \rightarrow E$

$$\begin{aligned} x &\rightarrow \sigma_A(x) = \sigma(x) && \text{si } x \in A \\ x &\rightarrow \sigma_A(x) = x && \text{si } x \notin A. \end{aligned}$$

#### Remarque 3-3-2 :

Soient  $E$  un ensemble,  $\sigma$  une permutation de  $E$  et  $A$  une partie de  $E$ .

1) Si  $A$  est finie alors  $A$  est une partie stable de  $E$  par  $\sigma$  si et seulement si  $\sigma(A) \subset A$ .

2) Si  $E$  est fini alors  $A$  est une partie stable de  $E$  par  $\sigma$  si et seulement si  $\sigma(A) \subset A$ .



**En effet :**

1) Supposons que  $A$  est finie.

$\Rightarrow$  ) **Si  $A$  est une partie stable de  $E$  par  $\sigma$  :**

Alors :  $\sigma(A) = A \subset A$ .

$\Leftarrow$  ) **Si  $\sigma(A) \subset A$  :**

Alors :  $\begin{cases} \sigma(A) \subset A \\ |\sigma(A)| = |A| \end{cases} \Rightarrow \sigma(A) = A$ . Donc  $A$  est une partie stable de  $E$  par  $\sigma$ .

2) Supposons que  $E$  est fini.

Puisque  $E$  est un ensemble fini et puisque  $A$  est une partie de  $E$  alors  $A$  est finie.

Par suite (d'après 1)),  $A$  est une partie stable de  $E$  par  $\sigma$  si et seulement si  $\sigma(A) \subset A$ .

### **Proposition 3-3-3 :**

Soient  $E$  un ensemble et  $\sigma$  une permutation de  $E$ .

Si  $A$  est une partie de  $E$ .stable par  $\sigma$  alors :

1)  $\sigma_A$  est une permutation de  $E$ .

2)  $\text{supp}\sigma_A \subset A$ .

3)  $A$  est une partie de  $E$ .stable par  $\sigma_A$ .

### **Démonstration :**

1)  $\star \forall x, y \in E$  tq :  $x \neq y$ .

- **Si  $x, y \in A$  :**

$\sigma_A(x) = \sigma(x) \neq \sigma(y) = \sigma_A(y) \Rightarrow \sigma_A(x) \neq \sigma_A(y)$ .

- **Si  $x, y \notin A$  :**

$\sigma_A(x) = x \neq y = \sigma_A(y) \Rightarrow \sigma_A(x) \neq \sigma_A(y)$ .

- **Si  $x \in A$  et  $y \notin A$  :**

$\begin{cases} \sigma_A(x) = \sigma(x) \in \sigma(A) = A \\ \sigma_A(y) = y \notin A \end{cases} \Rightarrow \sigma_A(x) \neq \sigma_A(y)$ .

- **Si  $x \notin A$  et  $y \in A$  :**

$\begin{cases} \sigma_A(x) = x \notin A \\ \sigma_A(y) = \sigma(y) \in \sigma(A) = A \end{cases} \Rightarrow \sigma_A(x) \neq \sigma_A(y)$ .

Donc  $\sigma_A$  injective.

$\star \forall y \in E$  :

- **Si  $y \in A$  :**

Alors :  $y \in A = \sigma(A) \Rightarrow [\exists x \in A \text{ tq : } \sigma(x) = y] \\ \Rightarrow [\exists x \in A \subset E \text{ tq : } \sigma_A(x) = y]$ .

- **Si  $y \notin A$  :**

Alors :  $\sigma_A(y) = y$ .

Donc  $\sigma_A$  surjective.

Ce qui montre que  $\sigma_A$  est une permutation de  $E$ .

2)  $\forall x \in C_E^A : x \notin A \Rightarrow \sigma_A(x) = x \Rightarrow x \notin \text{supp}\sigma_A \Rightarrow x \in C_E^{\text{supp}\sigma_A}$ .

Alors :  $C_E^A \subset C_E^{\text{supp}\sigma_A} \Rightarrow C_E^{\text{supp}\sigma_A} \subset C_E^{C_E^A} \Rightarrow \text{supp}\sigma_A \subset A$ .

3)  $\sigma_A(A) = \sigma(A) = A$ . Donc  $A$  est une partie de  $E$ .stable par  $\sigma_A$ .

**Exemple 3-3-4 :**

Pour  $n = 11$ , soient  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 9 & 7 & 10 & 4 & 6 & 3 & 8 & 11 & 5 & 2 \end{pmatrix}$ ,

$A = \{1, 2, 3, 7, 9, 11\}$  et  $B = \{3, 6, 7, 11\}$ .

1)  $A$  est stable par  $\sigma$

2)  $B$  n'est pas stable par  $\sigma$ .

3)  $\sigma_A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 9 & 7 & 4 & 5 & 6 & 3 & 8 & 11 & 10 & 2 \end{pmatrix}$ .

**Démonstration :**

1)  $\sigma(A) = \{\sigma(1), \sigma(2), \sigma(3), \sigma(9), \sigma(7), \sigma(11)\} = \{1, 9, 7, 11, 3, 2\} = \{1, 2, 3, 7, 9, 11\} = A$ .

Donc  $A$  est stable par  $\sigma$ .

2)  $\sigma(B) = \{\sigma(3), \sigma(6), \sigma(7), \sigma(11)\} = \{7, 6, 3, 2\} = \{2, 3, 7, 6\} \neq B$ .

Donc  $B$  n'est pas stable par  $\sigma$ .

3)  $\sigma_A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 & 5 & 6 & \sigma(7) & 8 & \sigma(9) & 10 & \sigma(11) \end{pmatrix}$   
 $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 9 & 7 & 4 & 5 & 6 & 3 & 8 & 11 & 10 & 2 \end{pmatrix}$ .

**Propriétés 3-3-5 :**

Soient  $E$  un ensemble,  $A$  une partie quelconque de  $E$ ,  $\mathcal{M} = \{\sigma \in S(E) \text{ tq : } \sigma(A) = A\}$

et  $\varphi_A$  l'application de  $\mathcal{M}$  vers  $\mathcal{M}$  lui même par :  $\varphi_A : \mathcal{M} \rightarrow \mathcal{M}$

$\sigma \mapsto \varphi_A(\sigma) = \sigma_A$ .

1)  $\mathcal{M}$  est un sous-groupe de  $S(E)$ .

2) Si  $\sigma$  est une permutation de  $E$  et si  $A$  est stable par  $\sigma$  alors :

a)  $\forall i \in \mathbb{Z} : A$  est stable par  $\sigma^i$ .

b)  $\forall \tau \in \langle \sigma \rangle : A$  est stable par  $\tau$ .

3)  $\varphi_A$  est un homomorphisme.

4) Si  $\sigma$  est une permutation de  $E$  et si  $A$  est stable par  $\sigma$  alors :

a)  $\forall i \in \mathbb{Z} : (\sigma^i)_A = (\sigma_A)^i$ .

b)  $\forall \tau \in \langle \sigma \rangle : \tau_A \in \langle \sigma_A \rangle$ .

**Démonstration :**

1) •  $e_E(A) = \{e_E(a) \text{ tq : } a \in A\} = \{a \text{ tq : } a \in A\} = A \Rightarrow e_E \in \mathcal{M} \Rightarrow \mathcal{M} \neq \emptyset$ .

•  $\forall \sigma, \tau \in \mathcal{M} : (\sigma\tau)(A) = \sigma(\tau(A)) = \sigma(A) = A \Rightarrow \sigma\tau \in \mathcal{M}$ .

•  $\forall \sigma \in \mathcal{M} : \sigma^{-1}(A) = \sigma^{-1}(\sigma(A)) = (\sigma^{-1}\sigma)(A) = e_E(A) = A \Rightarrow \sigma^{-1} \in \mathcal{M}$ .

Donc  $\mathcal{M}$  est un sous-groupe de  $S(E)$ .

2) Supposons que  $\sigma$  est une permutation de  $E$  et que  $A$  est stable par  $\sigma$ .

a)  $\forall i \in \mathbb{Z} :$

Puisque  $A$  est stable par  $\sigma$  alors  $\sigma \in \mathcal{M}$ . Donc  $\sigma^i \in \mathcal{M}$ .

Ce qui montre que  $A$  est stable par  $\sigma^i$ .

b)  $\forall \tau \in \langle \sigma \rangle : \exists i \in \mathbb{Z} \text{ tq : } \tau = \sigma^i$ .

Alors (d'après a))  $A$  est stable par  $\sigma^i = \tau$ .

3)  $\forall \sigma, \tau \in \mathcal{M}$  :

$\forall a \in E$  :

- **Si  $a \in A$  :**

$$\begin{aligned} [\varphi_A(\sigma\tau)](a) &= (\sigma\tau)_A(a) = (\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(\tau_A(a)) = \sigma_A(\tau_A(a)) \\ &= (\sigma_A\tau_A)(a) \\ &= [\varphi_A(\sigma)\varphi_A(\tau)](a). \end{aligned}$$

- **Si  $a \notin A$  :**

$$\begin{aligned} [\varphi_A(\sigma\tau)](a) &= (\sigma\tau)_A(a) = a = \tau_A(a) = \sigma_A(\tau_A(a)) \text{ (car } \tau_A(a) = a \notin A) \\ &= (\sigma_A\tau_A)(a) \\ &= [\varphi_A(\sigma)\varphi_A(\tau)](a). \end{aligned}$$

Donc  $\varphi_A(\sigma\tau) = \varphi_A(\sigma)\varphi_A(\tau)$ .

Ce qui prouve que  $\varphi_A$  est un homomorphisme.

4) Si  $\sigma$  est une permutation de  $E$  et si  $A$  est stable par  $\sigma$  alors :

a)  $\forall i \in \mathbb{Z}$  :

Puisque  $A$  est stable par  $\sigma$  alors  $\sigma \in \mathcal{M}$ .

Puisque  $\varphi_A$  est un homomorphisme de  $\mathcal{M}$  vers  $\mathcal{M}$  lui même alors,

$$(\sigma^i)_A = \varphi_A(\sigma^i) = \varphi_A(\sigma)^i = (\sigma_A)^i.$$

b)  $\forall \tau \in \langle \sigma \rangle : \exists i \in \mathbb{Z} \text{ tq : } \tau = \sigma^i.$

Alors (d'après a))  $\tau_A = (\sigma^i)_A = (\sigma_A)^i \in \langle \sigma_A \rangle.$

### Notation 3-3-6 :

Soient  $E$  un ensemble et  $\sigma$  une permutation de  $E$ . Si  $\sigma \neq e_E$  on note par  $R_\sigma$  la relation définie dans  $\text{supp}(\sigma)$  par :  $\forall x, y \in \text{supp}(\sigma) : \exists \tau \in \langle \sigma \rangle \text{ tq : } y = \tau(x).$

### Proposition 3-3-7 :

Soient  $E$  un ensemble et  $\sigma$  une permutation de  $E$ . Si  $\sigma \neq e_E$ ,  $R_\sigma$  est une relation d'équivalence dans  $\text{supp}(\sigma)$ .

#### Démonstration :

•  $\forall x \in \text{supp}(\sigma) : [e_E \in \langle \sigma \rangle \text{ et } x = e_E(x)] \Rightarrow xR_\sigma x$ . Donc  $R_\sigma$  est réflexive.

•  $\forall x, y \in \text{supp}(\sigma) \text{ tq : } xR_\sigma y$ . Il existe  $\tau \in \langle \sigma \rangle$  tel que  $y = \tau(x)$ .

Donc  $\tau^{-1} \in \langle \sigma \rangle$  et  $x = \tau^{-1}(y)$ , par suite  $yR_\sigma x$ .

Ce qui montre que  $R_\sigma$  est symétrique.

•  $\forall x, y, z \in \text{supp}(\sigma) \text{ tq : } \begin{cases} xR_\sigma y \\ yR_\sigma z \end{cases}$ . Il existe  $\tau, u \in \langle \sigma \rangle$  tel que  $\begin{cases} y = \tau(x) \\ z = u(y) \end{cases}$ .

Alors :  $u\tau \in \langle \sigma \rangle$  et  $z = u(y) = u(\tau(x)) = (u\tau)(x)$ . Donc :  $xR_\sigma z$ .

Ce qui montre que  $R_\sigma$  est transitive.

Puisque  $R_\sigma$  est réflexive, symétrique et transitive alors  $R_\sigma$  est une relation d'équivalence dans  $\text{supp}(\sigma)$ .

### Proposition et définition 3-3-8 :

Soient  $E$  un ensemble fini et  $\sigma$  une permutation de  $E$ . Si  $\sigma \neq e_E$  alors les quatres propriétés suivantes sont vérifiées :

1)  $\forall A \in \text{supp}(\sigma) \not\subset R_\sigma : A$  est stable par  $\sigma$ .

2)  $\forall A \in \text{supp}(\sigma) \not\subset R_\sigma : \sigma_A$  est un cycle de support  $A$ .

C'est à dire :  $\forall A \in \text{supp}(\sigma) \not\subset R_\sigma : \text{supp}\sigma_A = A$ .

- 3)  $\forall A \in \text{supp}(\sigma) \not\sim R_\sigma : \sigma_A$  est un cycle de support.A.  
4)  $\forall A, B \in \text{supp}(\sigma) \not\sim R_\sigma : A \neq B \Rightarrow \text{supp}\sigma_A \cap \text{supp}\sigma_B = \emptyset$ .  
5)  $\forall A, B \in \text{supp}(\sigma) \not\sim R_\sigma : A \neq B \Rightarrow \sigma_A \sigma_B = \sigma_B \sigma_A$ .  
6)  $\sigma = \prod_{A \in \text{supp}(\sigma) \not\sim R_\sigma} \sigma_A$ . Cette égalité est appelée la décomposition de  $\sigma$  en produit de cycles de supports disjoints.

**Démonstration :**

- 1)  $\forall A \in \text{supp}(\sigma) \not\sim R_\sigma :$   
 $\forall x \in A : \sigma(x) = \sigma(x) \Rightarrow x R_\sigma \sigma(x) \Rightarrow \sigma(x) \in A$ .  
Alors :  $\sigma(A) \subset A \Rightarrow \sigma(A) = A$  (car  $A$  est un ensemble fini).  
Donc  $A$  est stable par  $\sigma$ .
- 2)  $\forall A \in \text{supp}(\sigma) \not\sim R_\sigma :$   
 $\subset ) \forall x \in A : \begin{cases} x \in \text{supp}(\sigma) \Rightarrow \sigma(x) \neq x \\ \sigma_A(x) = \sigma(x) \end{cases} \Rightarrow \sigma_A(x) = \sigma(x) \neq x \Rightarrow x \in \text{supp}(\sigma_A)$ .  
Donc :  $A \subset \text{supp}(\sigma_A)$ .  
 $\supset )$  Supposons que  $\text{supp}(\sigma_A)$  n'est pas inclus dans  $A$ .  
Alors il existe un élément  $x \in \text{supp}(\sigma_A)$  tel que  $x \notin A$ .  
 $x \notin A \Rightarrow \sigma_A(x) = x \Rightarrow x \notin \text{supp}(\sigma_A)$ . Ce qui est absurde. Donc :  $\text{supp}(\sigma_A) \subset A$ .  
Ce qui montre que  $\text{supp}(\sigma_A) = A$ .
- 3)  $\forall A \in \text{supp}(\sigma) \not\sim R_\sigma :$   
 $\forall x, y \in \text{supp}(\sigma_A) : x, y \in A \Rightarrow x R_\sigma y \Rightarrow [\exists \tau \in \langle \sigma \rangle \text{ tq : } y = \tau(x)]$   
 $\Rightarrow [\exists i \in \mathbb{Z} \text{ tq : } y = \sigma^i(x)] \Rightarrow [\exists i \in \mathbb{Z} \text{ tq : } y = (\sigma_A)^i(x)]$   
 $\Rightarrow [\exists i \in \mathbb{Z} \text{ tq : } y = \sigma_A^i(x)] \Rightarrow [\exists \tau \in \langle \sigma_A \rangle \text{ tq : } y = \tau(x)]$ .  
Donc  $\sigma_A$  est un cycle de support.A.
- 4)  $\forall A, B \in \text{supp}(\sigma) \not\sim R_\sigma : A \neq B \Rightarrow A \cap B = \emptyset \Rightarrow \text{supp}(\sigma_A) \cap \text{supp}(\sigma_B) = \emptyset$ .  
5)  $\forall A, B \in \text{supp}(\sigma) \not\sim R_\sigma : A \neq B \Rightarrow \text{supp}(\sigma_A) \cap \text{supp}(\sigma_B) = \emptyset$  (d'après 4))  
 $\Rightarrow \sigma_A \sigma_B = \sigma_B \sigma_A$ .
- 6) – **Si  $\text{supp}(\sigma) \not\sim R_\sigma$  contient un seul élément  $M$  :**  
 $\forall x \in E : - \text{Si } x \notin \text{supp}(\sigma) = M :$   

$$\sigma(x) = x = \sigma_M(x) = \left( \prod_{A \in \text{supp}(\sigma) \not\sim R_\sigma} \sigma_A \right)(x).$$
- **Si  $x \in \text{supp}(\sigma) = M$  :**  

$$\sigma(x) = x = \sigma_M(x) = \left( \prod_{A \in \text{supp}(\sigma) \not\sim R_\sigma} \sigma_A \right)(x).$$
Donc :  $\sigma = \prod_{A \in \text{supp}(\sigma) \not\sim R_\sigma} \sigma_A$ .
- **Si  $\text{supp}(\sigma) \not\sim R_\sigma$  contient aux moins deux éléments :**  
 $\forall x \in E : - \text{Si } x \notin \text{supp}(\sigma) :$   
Alors :  $\forall A \in \text{supp}(\sigma) \not\sim R_\sigma : \sigma_A(x) = x$ .  
Donc :  $\sigma(x) = x = \left( \prod_{A \in \text{supp}(\sigma) \not\sim R_\sigma} \sigma_A \right)(x)$ .

- Si  $x \in \text{supp}(\sigma)$  :

Il existe un élément  $M \in \text{supp}(\sigma) \not\prec R_\sigma$  tq :  $x \in M$ .

$x \in M \Rightarrow \sigma_M(x) = \sigma(x)$ .

$\forall A \in \text{supp}(\sigma) \not\prec R_\sigma - \{M\} : x \notin M$  (car  $M \cap A = \emptyset$ )  $\Rightarrow \sigma_A(x) = x$ .

Par suite :  $\left( \prod_{A \in \text{supp}(\sigma) \not\prec R_\sigma - \{M\}} \sigma_A \right)(x) = x$ .

Donc :  $\sigma(x) = \sigma_M \left( \left( \prod_{A \in \text{supp}(\sigma) \not\prec R_\sigma - \{M\}} \sigma_A \right)(x) \right)$

$= \left( \sigma_M \prod_{A \in \text{supp}(\sigma) \not\prec R_\sigma - \{M\}} \sigma_A \right)(x)$

$= \left( \prod_{A \in \text{supp}(\sigma) \not\prec R_\sigma} \sigma_A \right)(x)$ .

Ce qui montre que :  $\sigma = \prod_{A \in \text{supp}(\sigma) \not\prec R_\sigma} \sigma_A$ .

### Corollaire 3-3-9 :

Soit  $E$  un ensemble fini. Si  $E$  contient au moins deux éléments alors on a les quatres propriétés suivantes :

- 1) Toute permutation de  $E$  se décompose en produit de cycles. C'est à dire toute permutation de  $E$  est un produit de cycles.
- 2) Le groupe  $S(E)$  est engendré par l'ensemble des cycles de  $E$ .
- 3) Toute permutation de  $E$  se décompose en produit de transpositions. C'est à dire toute permutation de  $E$  est un produit de transpositions.
- 4) Le groupe  $S(E)$  est engendré par l'ensemble des transpositions de  $E$ .

### Démonstration :

- 1) Soit  $\sigma$  une permutation quelconque de  $E$ .

- Si  $\sigma = e_E$  :

Soient  $a$  et  $b$  deux éléments quelconques distincts de  $E$ .

$\sigma = e_E = (a, b)(a, b)$  se décompose en produit des deux cycles  $(a, b)$  et  $(a, b)$ .

- Si  $\sigma \neq e_E$  :

D'après la proposition précédente,  $\sigma$  se décompose en produit de cycles.

- 2) Puisque tous les éléments de  $S(E)$  se décomposent en produit de cycles alors le groupe  $S(E)$  est engendré par l'ensemble des cycles de  $E$ .
- 3) Puisque toute permutation de  $E$  se décompose en produit de cycles et puisque tout cycle se décompose en produit de transpositions alors toute permutation de  $E$  se décompose en produit de transpositions.
- 4) Puisque tous les éléments de  $S(E)$  se décomposent en produit de transpositions alors le groupe  $S(E)$  est engendré par l'ensemble des transpositions de  $E$ .

**Définition 3-3-10 :**

Soient  $E$  un ensemble,  $\sigma$  une permutation de  $E$  et  $k_1, \dots, k_r$  des entiers naturels tels que  $k_1 \geq \dots \geq k_r \geq 2$ . On dit que  $\sigma$  est de type  $(k_1, \dots, k_r)$  s'il existe des cycles  $\sigma_1, \dots, \sigma_r$  de type respectivement  $k_1, \dots, k_r$  de supports disjoints deux à deux tels que :

$$\sigma = \sigma_1 \dots \sigma_r.$$

**Théorème 3-3-11 :**

Soit  $E$  un ensemble fini. Toute une permutation de  $E$  distinct de  $e_E$  admet un type et un seul.

**Démonstration :**

Soit  $\sigma$  une permutation de  $E$  distinct de  $e_E$ .

**- Existence :**

Soient  $A_1, \dots, A_r$  les éléments de  $\text{supp}(\sigma) \setminus R_\sigma$  tels que  $|A_1| \geq \dots \geq |A_r|$ .

$\forall i = 1, \dots, r$  : posons  $k_i = |A_i|$  et  $\sigma_i = \sigma_{A_i}$ .

Puisque  $\sigma_{A_i}$  est un cycle de support  $A_i$  alors :  $k_i = |A_i| \geq 2$ .

Alors  $k_1 \geq \dots \geq k_r \geq 2$  et  $\sigma_1, \dots, \sigma_r$  des cycles de supports  $A_1, \dots, A_r$  disjoints deux à deux tels que  $\sigma = \prod_{A \in \text{supp}(\sigma) \setminus R_\sigma} \sigma_A = \sigma_{A_1} \dots \sigma_{A_r} = \sigma_1 \dots \sigma_r$ .

Donc  $\sigma$  est de type  $(k_1, \dots, k_r)$ .

**- Unicité :**

Soit  $(h_1, \dots, h_s)$  un autre type de  $\sigma$ .

Alors  $h_1 \geq \dots \geq h_s \geq 2$  et il existe des cycles  $\tau_1, \dots, \tau_s$  de types  $h_1, \dots, h_s$  de support disjoints deux à deux tels que  $\sigma = \tau_1 \dots \tau_s$ .

$\forall i = 1, \dots, s$  : posons  $B_i = \text{supp}(\tau_i)$ .

Montrons que :  $\{A_1, \dots, A_r\} = \{B_1, \dots, B_s\}$ .

Posons  $U = \{A_1, \dots, A_r\}$  et  $V = \{B_1, \dots, B_s\}$ .  $U$  et  $V$  sont deux partitions de  $\text{supp}(\sigma)$ .

$\subset$ )  $\forall i = 1, \dots, r$  :

Soit  $a \in A_i$ .

Puisque  $V$  est une partition de  $\text{supp}(\sigma)$  alors il existe  $j = 1, \dots, s$  tel que  $a \in B_j$ .

Montrons que  $A_i = B_j \in V$ .

$\forall x \in \text{supp}(\sigma)$  :

$$x \in A_i \Leftrightarrow x R_\sigma a \Leftrightarrow \exists p \in \mathbb{Z} \text{ tq : } x = \sigma^p(a) = (\tau_1 \dots \tau_s)^p(a) = (\tau_1^p \dots \tau_s^p)(a) = \tau_j^p(a)$$

$$\Leftrightarrow x \in B_j.$$

Donc  $A_i = B_j \in V$ .

Alors :  $U \subset V$ .

$\supset$ )  $\forall j = 1, \dots, s$  :

Soit  $b \in B_j$ . Puisque  $U$  est une partition de  $\text{supp}(\sigma)$  alors il existe  $i = 1, \dots, r$  tel que  $b \in A_i$ .

Montrons que  $B_j = A_i$ .

$$\forall x \in \text{supp}(\sigma) : x \in B_j \Leftrightarrow \exists p \in \mathbb{Z} \text{ tq : } x = (\tau_j)^p(a) = (\tau_1^p \dots \tau_s^p)(a) = (\tau_1 \dots \tau_s)^p(a) = \sigma^p(a)$$

$$\Leftrightarrow x R_\sigma a$$

$$\Leftrightarrow x \in A_i.$$

Donc  $B_j = A_i \in U$ .

Alors :  $V \subset U$ .

Par suite :  $\{A_1, \dots, A_r\} = U = V = \{B_1, \dots, B_s\}$ .

Ce qui montre que :  $\begin{cases} r = s \\ (k_1, \dots, k_r) = (|A_1|, \dots, |A_r|) = (|B_1|, \dots, |B_r|) = (h_1, \dots, h_r) \end{cases}$ .

### Proposition 3-3-12 :

Soit  $E$  un ensemble fini. Si  $\sigma$  est une permutation de  $E$  de type  $(k_1, \dots, k_r)$  alors l'ordre de  $\sigma$  est égal au p.p.c.m de  $k_1, \dots, k_r$  (c'est à dire  $|\sigma| = \bigvee_{i=1}^r k_i$ ).

### Démonstration :

Si  $\sigma$  est une permutation de  $E$  de type  $(k_1, \dots, k_r)$  alors il existe des cycles  $\sigma_1, \dots, \sigma_r$  de type respectivement  $k_1, \dots, k_r$  de supports disjoints deux à deux tels que :

$$\sigma = \sigma_1 \dots \sigma_r.$$

Puisque  $\sigma_1, \dots, \sigma_r$  sont des permutations de  $E$  de supports disjoints deux à deux alors :

$$|\sigma| = |\sigma_1 \dots \sigma_r| = \bigvee_{i=1}^r |\sigma_i| = \bigvee_{i=1}^r k_i.$$

### Exemple 3-3-13 :

Soit  $E$  un ensemble fini.

★ Pour  $n = 18$ , soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 5 & 7 & 2 & 1 & 8 & 9 & 10 & 4 & 18 & 15 & 6 & 3 & 13 & 16 & 12 & 14 & 17 & 11 \end{pmatrix}$$

$$\text{On a : } \begin{cases} \sigma(1) = 5, & \sigma(5) = 8, & \sigma(8) = 4, & \sigma(4) = 1 \\ \sigma(2) = 7, & \sigma(7) = 10, & \sigma(10) = 15, & \sigma(15) = 12, & \sigma(12) = 3, & \sigma(3) = 2 \\ \sigma(6) = 9, & \sigma(9) = 18, & \sigma(18) = 11, & \sigma(11) = 6 \\ \sigma(14) = 16, & \sigma(16) = 14 \\ \sigma(13) = 13, & \sigma(17) = 17 \end{cases}$$

$$\text{Donc : } \sigma = (1, 5, 8, 4)(2, 7, 10, 15, 12, 3)(6, 9, 18, 11)(14, 16)$$

$$= (2, 7, 10, 15, 12, 3)(1, 5, 8, 4)(6, 9, 18, 11)(14, 16).$$

Ce qui montre que  $\sigma$  est de type  $(6, 4, 4, 2)$  et  $\sigma$  est d'ordre  $6 \vee 4 \vee 4 \vee 2 = 12$ .

★ Pour tout entier naturel  $k \geq 2$ , les permutations de  $E$  de type  $(k)$  sont les  $k$ -cycles.

★ Les permutations de  $E$  de type  $(2)$  sont les transpositions.

## 3-4-Signature d'une permutation :

### Définition 3-4-1 :

Soient  $E$  un ensemble fini et  $\sigma$  une permutation de  $E$ .

- Si  $\sigma \neq e_E$  de type  $(k_1, \dots, k_r)$  :

On appelle signature de  $\sigma$  le nombre noté  $\varepsilon(\sigma)$  défini par :

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^r k_i - r} = (-1)^{k_1 + \dots + k_r - r}$$

- Si  $\sigma = e_E$  :

On dit que  $\sigma = e_E$  est de signature 1 et on note  $\varepsilon(e_E) = 1$ .

- Si  $\varepsilon(\sigma) = 1$  :

On dit que  $\sigma$  est paire.

- Si  $\varepsilon(\sigma) = -1$  :

On dit que  $\sigma$  est impaire.

### Notation 3-4-2 :

Si  $E$  est un ensemble fini alors l'ensemble des permutations paires de  $E$  est noté  $A(E)$ . En particulier si  $n$  est un entier naturel non nul et si  $E = \{1, \dots, n\}$ , alors  $A(E)$  est noté  $A_n$ .

### Exemple 3-4-3 :

Soit  $E$  un ensemble fini.

1) Pour  $n = 18$ , soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 5 & 7 & 2 & 1 & 8 & 9 & 10 & 4 & 18 & 15 & 6 & 3 & 13 & 16 & 12 & 14 & 17 & 11 \end{pmatrix}$$

On a vu que  $\sigma$  est de type  $(6, 4, 4, 2)$ . Donc  $\varepsilon(\sigma) = (-1)^{6+4+4+2-4} = (-1)^{12} = 1$

Donc  $\sigma$  est paire.

2) Si  $\sigma$  est une permutation de  $E$  de type  $(4, 2, 2)$ . alors :

$\varepsilon(\sigma) = (-1)^{4+2+2-3} = (-1)^5 = -1$  Donc  $\sigma$  est impaire.

3) Pour tout entier naturel  $k \geq 2$ , les  $k$ -cycles de  $E$  sont des permutations de signature  $(-1)^{k-1}$ . C'est à dire si  $k \geq 2$  et si  $\sigma$  est un  $k$ -cycles de  $E$  alors  $\varepsilon(\sigma) = (-1)^{k-1}$ .

4) Les transpositions de  $E$  sont tous impaires. C'est à die si  $\sigma$  est une transposition de  $E$  alors  $\varepsilon(\sigma) = -1$ .

5) Soient  $k$  un entier naturel tel que  $k \geq 2$  et  $\sigma$  un  $k$ -cycle de  $E$ .

- Si  $k$  est paire alors  $\sigma$  est impaire.
- Si  $k$  est impaire alors  $\sigma$  est paire.
- $\sigma$  est paire si seulement si  $k$  est impaire.
- $\sigma$  est impaire si seulement si  $k$  est paire.

### Popriétés 3-4-4 :

Soit  $E$  un ensemble fini.

1)  $\varepsilon$  est une application de  $S(E)$  vers l'ensemble  $\{1, -1\}$  (qui est surjective si seulement si  $|E| \geq 2$ ).

2) Pour tout entier naturel non nul  $n$ ,  $\varepsilon$  est une application de  $S_n$  vers l'ensemble  $\{1, -1\}$  (qui est surjective si seulement si  $n \neq 1$ ).

3) Si  $M$  est un ensemble non vide de cycles de  $E$  de supports disjoints deux à deux

alors  $M$  est fini et  $\varepsilon\left(\prod_{\sigma \in M} \sigma\right) = \prod_{\sigma \in M} \varepsilon(\sigma)$ .

4) Si  $\sigma_1, \dots, \sigma_r$  sont des cycles de  $E$  de supports disjoints deux à deux alors :

$$\varepsilon\left(\prod_{i=1}^r \sigma_i\right) = \prod_{i=1}^r \varepsilon(\sigma_i).$$

5) Si  $\sigma$  et  $\tau$  sont des permutations de  $E$  de supports disjoints alors :  $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ .

6) Si  $a_1, \dots, a_k, a_{k+1}$  sont des éléments de  $E$  distincts deux à deux alors :

$$\varepsilon((a_1, \dots, a_k)(a_k, a_{k+1})) = -\varepsilon((a_1, \dots, a_k)).$$



- 7) Soient  $a_1, \dots, a_k$  des éléments de  $E$  distincts deux à deux.
- i)  $\varepsilon((a_1, \dots, a_k)(a_1, a_2)) = -\varepsilon((a_1, \dots, a_k))$ .
  - ii)  $\varepsilon((a_1, \dots, a_k)(a_1, a_k)) = -\varepsilon((a_1, \dots, a_k))$ .
  - iii) Si  $k \geq 3$  et si  $2 < r < k$  alors :  $\varepsilon((a_1, \dots, a_k)(a_1, a_r)) = -\varepsilon((a_1, \dots, a_k))$ .
- 8) Si  $\sigma$  est un cycle de  $E$  et si  $u$  est une transposition de  $E$  alors  $\varepsilon(\sigma u) = -\varepsilon(\sigma)$ .
- 9) Soient  $\sigma, \tau$  deux cycles de  $E$  de supports disjoints et  $u$  une transposition de  $E$ .
- 10) Si  $\sigma$  est une permutation de  $E$  et si  $u$  est une transposition de  $E$  alors  $\varepsilon(\sigma u) = -\varepsilon(\sigma)$ .

### Démonstration :

1) •  $\forall \sigma \in S(E)$  :

- Si  $\sigma = e_E$  :

$$\varepsilon(\sigma) = \varepsilon(e_E) = 1 \in \{1, -1\}.$$

- Si  $\sigma \neq e_E$  :

$$\sum_{i=1}^r k_i - r$$

Soit  $(k_1, \dots, k_r)$  le type de  $\sigma$ .  $\varepsilon(\sigma) = (-1)^{\sum_{i=1}^r k_i - r} \in \{1, -1\}$ .

Donc  $\varepsilon$  est une application de  $S(E)$  vers l'ensemble  $\{1, -1\}$ .

• - Si  $|E| = 0$  ou  $|E| = 1$  :

Alors  $S(E) = \{e_E\}$ . Par suite  $\varepsilon(S(E)) = \varepsilon(\{e_E\}) = \{\varepsilon(e_E)\} = \{1\} \neq \{1, -1\}$ .

Donc  $\varepsilon$  n'est pas une application surjective de  $S(E)$  vers l'ensemble  $\{1, -1\}$ .

- Si  $|E| \geq 2$  :

Soient  $a$  et  $b$  deux éléments distincts de  $E$ .

$$\begin{cases} \varepsilon(e_E) = 1 \\ \varepsilon((a, b)) = -1 \end{cases} \Rightarrow 1, -1 \in \varepsilon(S(E)) \Rightarrow \{1, -1\} \subset \varepsilon(S(E)) \Rightarrow \varepsilon(S(E)) = \{1, -1\}.$$

Donc  $\varepsilon$  est une application surjective de  $S(E)$  vers l'ensemble  $\{1, -1\}$ .

Ce qui montre que  $\varepsilon$  est une application de  $S(E)$  vers l'ensemble  $\{1, -1\}$  qui est surjective si et seulement si  $|E| \geq 2$ .

2) Soit  $n$  un entier naturel non nul. Pour  $E = \{1, \dots, n\}$  on a :

•  $\varepsilon$  est une application de  $S_n$  vers l'ensemble  $\{1, -1\}$ .

•  $[\varepsilon \text{ est surjective}] \Leftrightarrow n = |E| \geq 2$ . (d'après 1))  $\Leftrightarrow n \neq 1$  (car  $n \neq 0$ ).

3) Supposons que  $M$  est un ensemble non vide de cycles de  $E$  de supports disjoints deux à deux.

Puisque  $E$  est fini alors  $S(E)$  est d'ordre fini et par suite  $M$  est fini (car  $M \subset S(E)$ ).

Soient  $\sigma_1, \dots, \sigma_r$  les éléments de  $M$  tels que  $|\sigma_1| \geq \dots \geq |\sigma_r|$ .

Pour tout  $i = 1, \dots, r$  : posons  $|\sigma_i| = k_i$ .

Alors  $\prod_{\sigma \in M} \sigma = \prod_{i=1}^r \sigma_i$  est de type  $(k_1, \dots, k_r)$ .

$$\begin{aligned} \text{Donc : } \varepsilon\left(\prod_{\sigma \in M} \sigma\right) &= (-1)^{\sum_{i=1}^r k_i - r} = (-1)^{\sum_{i=1}^r (k_i - 1)} = \prod_{i=1}^r (-1)^{k_i - 1} = \prod_{i=1}^r \varepsilon(\sigma_i) \\ &= \prod_{\sigma \in M} \varepsilon(\sigma). \end{aligned}$$

4) Soient  $\sigma_1, \dots, \sigma_r$  des cycles de  $E$  de supports disjoints deux à deux.

Posons  $M = \{\sigma_1, \dots, \sigma_r\}$  alors (d'après la propriété précédente) :

$$\varepsilon\left(\prod_{i=1}^r \sigma_i\right) = \varepsilon\left(\prod_{\sigma \in M} \sigma\right) = \prod_{\sigma \in M} \varepsilon(\sigma) = \prod_{i=1}^r \varepsilon(\sigma_i).$$

5) Soient  $\sigma$  et  $\tau$  deux permutations de  $E$  de supports disjoints.

- Si  $\sigma = e_E$  :  $\varepsilon(\sigma\tau) = \varepsilon(e_E\tau) = \varepsilon(\tau) = 1\varepsilon(\tau) = \varepsilon(e_E)\varepsilon(\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ .
- Si  $\tau = e_E$  :  $\varepsilon(\sigma\tau) = \varepsilon(\sigma e_E) = \varepsilon(\sigma) = \varepsilon(\sigma)1 = \varepsilon(\sigma)\varepsilon(e_E) = \varepsilon(\sigma)\varepsilon(\tau)$ .
- Si  $\sigma \neq e_E$  et si  $\tau \neq e_E$  :

Puisque  $\sigma$  et  $\tau$  sont des permutations de  $E$  de supports disjoints alors il existe des cycles  $\sigma_1, \dots, \sigma_r, \tau_1, \dots, \tau_s$  de  $E$  de supports disjoints deux à deux tels

$$\text{que : } \sigma = \prod_{i=1}^r \sigma_i = \sigma_1 \dots \sigma_r \quad \text{et} \quad \tau = \prod_{i=1}^s \tau_i = \tau_1 \dots \tau_s.$$

Ce qui montre (d'après la propriété précédente) que :

$$\begin{aligned} \varepsilon(\sigma\tau) &= \varepsilon\left(\left(\prod_{i=1}^r \sigma_i\right)\left(\prod_{i=1}^s \tau_i\right)\right) = \prod_{i=1}^r \varepsilon(\sigma_i) \prod_{i=1}^s \varepsilon(\tau_i) = \varepsilon\left(\prod_{i=1}^r \sigma_i\right) \varepsilon\left(\prod_{i=1}^s \tau_i\right) \\ &= \varepsilon(\sigma)\varepsilon(\tau). \end{aligned}$$

6) Soient  $a_1, \dots, a_k, a_{k+1}$  des éléments de  $E$  distincts deux.

$$\begin{aligned} \varepsilon((a_1, \dots, a_k)(a_k, a_{k+1})) &= \varepsilon((a_1, \dots, a_k, a_{k+1})) = (-1)^{k+1-1} = (-1)^k = -(-1)^{k-1} \\ &= -\varepsilon((a_1, \dots, a_k)). \end{aligned}$$

7) i) - Si  $k = 2$  :

$$\begin{aligned} \varepsilon((a_1, \dots, a_k)(a_1, a_2)) &= \varepsilon((a_1, a_2)(a_1, a_2)) = \varepsilon(e_E) = 1 = (-1)(-1) \\ &= [\varepsilon(a_1, a_2)][\varepsilon(a_1, a_2)] = (-1)[\varepsilon(a_1, a_2)] = -[\varepsilon(a_1, a_2)] \\ &= -\varepsilon((a_1, \dots, a_k)). \end{aligned}$$

- Si  $k \neq 2$  :

Puisque  $(a_1, \dots, a_k)(a_1, a_2) = (a_1, a_3, \dots, a_k)$  est un  $(k-1)$ -cycle alors :

$$\varepsilon((a_1, \dots, a_k)(a_1, a_2)) = (-1)^{k-1-1} = -(-1)^{k-1} = -\varepsilon((a_1, \dots, a_k)).$$

ii) - Si  $k = 2$  :

D'après i) on a :

$$\varepsilon((a_1, \dots, a_k)(a_1, a_k)) = \varepsilon((a_1, \dots, a_k)(a_1, a_2)) = -\varepsilon((a_1, \dots, a_k)).$$

- Si  $k \neq 2$  :

$$\begin{aligned} \varepsilon((a_1, \dots, a_k)(a_1, a_k)) &= \varepsilon((a_k, a_1, \dots, a_{k-1})(a_k, a_1)) = -\varepsilon((a_k, a_1, \dots, a_{k-1})) \\ &= -\varepsilon((a_1, \dots, a_k)). \end{aligned}$$

iii) Supposons que  $k \geq 3$  et que  $2 < r < k$ .

$$\begin{aligned} \varepsilon((a_1, \dots, a_k)(a_1, a_r)) &= \varepsilon((a_1, a_{r+1}, \dots, a_k)(a_2, \dots, a_r)) \\ &= \varepsilon((a_{r+1}, \dots, a_k, a_1)(a_2, \dots, a_r)) = (-1)^{k-r+1+r-1-2} \\ &= (-1)^{k-2} = 1(-1)^{k-2} = (-1)^2(-1)^{k-2} = (-1)^k = -(-1)^{k-1} \\ &= -\varepsilon((a_1, \dots, a_k)). \end{aligned}$$

8) Supposons que  $\sigma$  est un cycle de  $E$  et que  $u$  est une transposition de  $E$ .

• Si  $\sigma$  et  $u$  de supports disjoints :

$$\text{Alors : } \varepsilon(\sigma u) = \varepsilon(\sigma)\varepsilon(u) = \varepsilon(\sigma)(-1) = -\varepsilon(\sigma).$$

• Si  $\text{supp}(\sigma) \cap \text{supp}(u)$  est un singleton :

Alors il existe des éléments  $a_1, \dots, a_k, a_{k+1}$  de  $E$  distincts deux à deux tels que :

$$\sigma = (a_1, \dots, a_k) \text{ et } u = (a_k, a_{k+1}).$$

$$\text{Alors : } \varepsilon(\sigma u) = \varepsilon((a_1, \dots, a_k)(a_k, a_{k+1})) = -\varepsilon((a_1, \dots, a_k)) = -\varepsilon(\sigma).$$

• Si  $\text{supp}(u) \subset \text{supp}(\sigma)$  :

Alors il existe des éléments  $a_1, \dots, a_k$  de  $E$  distincts deux à deux et il existe

$$r = 2, \dots, k \text{ tels que : } \sigma = (a_1, \dots, a_k) \text{ et } u = (a_1, a_r).$$

- Si  $r = 2$  :

$$\text{Alors : } \varepsilon(\sigma u) = \varepsilon((a_1, \dots, a_k)(a_1, a_2)) = -\varepsilon((a_1, \dots, a_k)) = -\varepsilon(\sigma).$$

- Si  $r = k$  :

$$\text{Alors : } \varepsilon(\sigma u) = \varepsilon((a_1, \dots, a_k)(a_1, a_k)) = -\varepsilon((a_1, \dots, a_k)) = -\varepsilon(\sigma).$$

- Si  $2 < r < k$  :

$$\text{Alors : } \varepsilon(\sigma u) = \varepsilon((a_1, \dots, a_k)(a_1, a_r)) = -\varepsilon((a_1, \dots, a_k)) = -\varepsilon(\sigma).$$

9) - Si  $\text{supp}(\sigma)$  et  $\text{supp}(u)$  sont disjoints :

$$\text{supp}(\sigma) \cap \text{supp}(\tau u) \subset \text{supp}(\sigma) \cap [\text{supp}(\tau) \cup \text{supp}(u)]$$

$$\text{Alors : } \text{supp}(\sigma) \cap \text{supp}(\tau u) \subset [\text{supp}(\sigma) \cap \text{supp}(\tau)] \cup [\text{supp}(\sigma) \cap \text{supp}(u)] = \emptyset \cup \emptyset = \emptyset.$$

$$\text{Donc : } \text{supp}(\sigma) \cap \text{supp}(\tau u) = \emptyset.$$

$$\text{Par suite : } \varepsilon(\sigma \tau u) = \varepsilon(\sigma) \varepsilon(\tau u) = \varepsilon(\sigma) [-\varepsilon(\tau)] = -\varepsilon(\sigma) \varepsilon(\tau) = -\varepsilon(\sigma \tau).$$

- Si  $\text{supp}(\tau)$  et  $\text{supp}(u)$  sont disjoints :

$$\text{supp}(\tau) \cap \text{supp}(\sigma u) \subset \text{supp}(\tau) \cap [\text{supp}(\sigma) \cup \text{supp}(u)]$$

$$\text{Alors : } \text{supp}(\tau) \cap \text{supp}(\sigma u) \subset [\text{supp}(\tau) \cap \text{supp}(\sigma)] \cup [\text{supp}(\tau) \cap \text{supp}(u)] = \emptyset \cup \emptyset = \emptyset.$$

$$\text{Donc : } \text{supp}(\tau) \cap \text{supp}(\sigma u) = \emptyset.$$

$$\text{Par suite : } \varepsilon(\sigma \tau u) = \varepsilon(\tau \sigma u) = \varepsilon(\tau) \varepsilon(\sigma u) = \varepsilon(\tau) [-\varepsilon(\sigma)] = -\varepsilon(\tau) \varepsilon(\sigma) = -\varepsilon(\tau \sigma) = -\varepsilon(\sigma \tau).$$

- Si  $\text{supp}(\sigma) \cap \text{supp}(u)$  et  $\text{supp}(\tau) \cap \text{supp}(u)$  ne sont pas vides :

Puisque  $\text{supp}(\sigma) \cap \text{supp}(u)$  et  $\text{supp}(\tau) \cap \text{supp}(u)$  ne sont pas vides alors il existe des éléments  $a_1, \dots, a_k, b_1, \dots, b_h$  de  $E$  distincts deux à deux tels que :

$$\sigma = (a_1, \dots, a_k), \quad \tau = (b_1, \dots, b_h) \quad \text{et} \quad u = (a_k, b_h).$$

$$\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset \Rightarrow \varepsilon(\sigma \tau) = \varepsilon(\sigma) \varepsilon(\tau) = (-1)^{k-1} (-1)^{h-1} = (-1)^{k+h-2}.$$

$$\begin{aligned} \sigma \tau u &= (a_1, \dots, a_k)(b_1, \dots, b_h)(a_k, b_h) = (a_1, \dots, a_k)(b_1, \dots, b_h)(b_h, a_k) \\ &= (a_1, \dots, a_k)(b_1, \dots, b_h, a_k) = (a_1, \dots, a_k)(a_k, b_1, \dots, b_h) \\ &= (a_1, \dots, a_k, b_1, \dots, b_h) \text{ est un } (k+h)\text{-cycle.} \end{aligned}$$

$$\text{Donc : } \varepsilon(\sigma \tau u) = (-1)^{k+h-1} = (-1)^{k+h-2+1} = -(-1)^{k+h-2} = -\varepsilon(\sigma \tau).$$

10) Soient  $\sigma$  une permutation de  $E$  et si  $u$  est une transposition de  $E$ .

- Si  $\sigma = e_E$  :

$$\text{Alors : } \varepsilon(\sigma u) = \varepsilon(e_E u) = \varepsilon(u) = -1 = -\varepsilon(e_E) = -\varepsilon(\sigma).$$

- Si  $\sigma \neq e_E$  et si  $\text{supp}(\sigma) \not\subset R_\sigma$  contient un seul élément :

Alors  $\text{supp}(\sigma)$  est le seul élément de  $\text{supp}(\sigma) \not\subset R_\sigma$  et  $\sigma$  est un cycle.

$$\text{Donc : } \varepsilon(\sigma u) = -\varepsilon(\sigma).$$

- Si  $\sigma \neq e_E$  et si le nombre des éléments de  $\text{supp}(\sigma) \not\subset R_\sigma$  est 2 :

Soient  $A_1$  et  $A_2$  les éléments de  $\text{supp}(\sigma) \not\subset R_\sigma$ .

Donc  $\sigma_{A_1}$  et  $\sigma_{A_2}$  sont des cycles de  $E$  de supports disjoints et  $\sigma = \sigma_{A_1} \sigma_{A_2}$ .

$$\text{Ce qui montre que : } \varepsilon(\sigma u) = \varepsilon(\sigma_{A_1} \sigma_{A_2} u) = -\varepsilon(\sigma_{A_1} \sigma_{A_2}) = -\varepsilon(\sigma).$$

- Si  $\sigma \neq e_E$  et si  $\text{supp}(\sigma) \not\subset R_\sigma$  contient au moins trois éléments :

Alors il existent deux éléments  $A_1$  et  $A_2$  de  $\text{supp}(\sigma) \not\subset R_\sigma$  distincts tels que  $\text{supp}(u)$  soit disjoint à tous les éléments de  $\text{supp}(\sigma) \not\subset R_\sigma - \{A_1, A_2\}$ .

Soient  $B_1, \dots, B_r$  les éléments de  $\text{supp}(\sigma) \not\subset R_\sigma - \{A_1, A_2\}$ .

$$\text{Donc : } \text{supp}(\sigma) \not\subset R_\sigma = \{B_1, \dots, B_r, A_1, A_2\}.$$

$$\text{Posons } \sigma_0 = \prod_{i=1}^r \sigma_{B_i}, \quad \sigma_1 = \sigma_{A_1} \text{ et } \sigma_2 = \sigma_{A_2}. \text{ On a : } \sigma = \sigma_0 \sigma_1 \sigma_2.$$

$$\text{supp}(\sigma_0) \cap \text{supp}(\sigma_1 \sigma_2 u) \subset \text{supp}(\sigma_0) \cap [\text{supp}(\sigma_1 \sigma_2) \cup \text{supp}(u)]. \text{ Par suite on a :}$$

$$\text{supp}(\sigma_0) \cap \text{supp}(\sigma_1 \sigma_2 u) \subset [\text{supp}(\sigma_0) \cap \text{supp}(\sigma_1 \sigma_2)] \cup [\text{supp}(\sigma_0) \cap \text{supp}(u)] = \emptyset.$$

Ce qui montre que :

$$\begin{aligned} \varepsilon(\sigma u) &= \varepsilon(\sigma_0 \sigma_1 \sigma_2 u) = \varepsilon(\sigma_0) \varepsilon(\sigma_1 \sigma_2 u) = \varepsilon(\sigma_0) [-\varepsilon(\sigma_1 \sigma_2)] = -\varepsilon(\sigma_0) \varepsilon(\sigma_1 \sigma_2) \\ &= -\varepsilon(\sigma_0 \sigma_1 \sigma_2) = -\varepsilon(\sigma). \end{aligned}$$

**Lemme 3-4-4 :**

Si  $E$  est un ensemble fini et si  $\sigma_1, \dots, \sigma_r$  sont des transpositions de  $E$  alors :

$$\varepsilon\left(\prod_{i=1}^r \sigma_i\right) = (-1)^r.$$

**Démonstration :**

Montrons par récurrence que pour tout entier naturel non nul  $r$ , si  $\sigma_1, \dots, \sigma_r$  sont des

transpositions de  $E$  alors :  $\varepsilon\left(\prod_{i=1}^r \sigma_i\right) = (-1)^r$ .

**- Pour  $r = 1$  :**

Si  $\sigma_1$  est une transposition de  $E$  alors :

$$\varepsilon\left(\prod_{i=1}^r \sigma_i\right) = \varepsilon\left(\prod_{i=1}^1 \sigma_i\right) = \varepsilon(\sigma_1) = -1 = (-1)^1 = (-1)^r.$$

**- Pour  $r - 1$  :**

Supposons que si  $\sigma_1, \dots, \sigma_{r-1}$  sont des transpositions de  $E$  alors :

$$\varepsilon\left(\prod_{i=1}^{r-1} \sigma_i\right) = (-1)^{r-1}.$$

**- Pour  $r$  :**

Montrons qu'alors si  $\sigma_1, \dots, \sigma_r$  sont des transpositions de  $E$  alors :

$$\varepsilon\left(\prod_{i=1}^r \sigma_i\right) = (-1)^r.$$

Soient  $\sigma_1, \dots, \sigma_r$  sont des transpositions de  $E$ .

$$\varepsilon\left(\prod_{i=1}^r \sigma_i\right) = \varepsilon\left(\left(\prod_{i=1}^{r-1} \sigma_i\right)\sigma_r\right) = -\varepsilon\left(\prod_{i=1}^{r-1} \sigma_i\right) = -(-1)^{r-1} = (-1)^r.$$

**Théorème 3-4-5 :**

Si  $E$  est un ensemble fini alors l'application  $\varepsilon$  est un homomorphisme du groupe  $(S(E), \cdot)$  vers le groupe multiplicatif  $\{1, -1\}$ .

**Démonstration :**

Soient  $\sigma$  et  $\tau$  deux permutations quelconques de  $E$ .

Il des transpositions  $\sigma_1, \dots, \sigma_r, \tau_1, \dots, \tau_s$  tels que :  $\sigma = \sigma_1 \dots \sigma_r$  et  $\tau = \tau_1 \dots \tau_s$ .

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma_1, \dots, \sigma_r, \tau_1, \dots, \tau_s) = (-1)^{r+s} = (-1)^r (-1)^s = \varepsilon(\sigma)\varepsilon(\tau).$$

Donc  $\varepsilon$  est un homomorphisme du groupe  $(S(E), \cdot)$  vers le groupe multiplicatif  $\{1, -1\}$ .

**Corollaire 3-4-6 :**

Si  $E$  est un ensemble fini alors  $A(E) = \ker \varepsilon$  est un sous groupe de  $S(E)$ .

En particulier si  $n$  est un entier naturel non nul alors  $A_n = \ker \varepsilon$  est un sous groupe de  $S_n$ .

**Lemme 3-4-7 :**

Si  $E$  est un ensemble fini et si  $\tau$  est une permutation impaire de  $E$  alors :

$$A(E) \neq \tau A(E) \text{ et } S(E) \not\subset A(E) = \{A(E), \tau A(E)\}.$$

En particulier si  $n$  est un entier naturel non nul alors :

$$A_n \neq \tau A_n \text{ et } S_n \not\subset A_n = \{A_n, \tau A_n\}.$$

**En effet :**

Puisque  $\tau \notin A(E)$  (car  $\tau$  est une permutation impaire de  $E$ ) alors  $A(E) \neq \tau A(E)$ .

$$\forall A \in [S(E) \not\subset A(E)] : \exists \sigma \in S(E) \text{ tq } A = \sigma A(E).$$

**- Si  $\sigma$  est paire :**

$$\text{Alors : } \sigma \in A(E) \Rightarrow A = \sigma A(E) = A(E).$$

**- Si  $\sigma$  est impaire :**

$$\text{Alors : } \varepsilon(\tau^{-1}\sigma) = \varepsilon(\tau)^{-1}\varepsilon(\sigma) = (-1)^{-1}(-1) = (-1)(-1) = 1 \Rightarrow \tau^{-1}\sigma \in A(E).$$

$$\text{Donc : } \sigma \in \tau A(E) \Rightarrow A = \sigma A(E) = \tau A(E).$$

Ce qui montre que :  $S(E) \not\subset A(E) = \{A(E), \tau A(E)\}.$

**Théorème 3-4-8 :**

Soit  $E$  est un ensemble fini de cardinal  $n$ .

- Si  $n = 1$  alors  $A(E) = S(E)$  est un groupe d'ordre 1.

En particulier  $A_1 = S_1$  est un groupe d'ordre 1.

- Si  $n \geq 2$  alors  $[S(E) : A(E)] = 2$  et  $|A(E)| = \frac{n!}{2}.$

En particulier  $[S_n : A_n] = 2$  et  $|A_n| = \frac{n!}{2}.$

**Démonstration :****- Si  $n = 1$  :**

$$|S(E)| = 1! = 1. \text{ Donc } A(E) = S(E) \text{ est un groupe d'ordre 1.}$$

**- Si  $n \geq 2$  :**

Alors  $E$  contient au moins deux éléments  $a$  et  $b$  distincts. Par suite la transposition  $\tau = (a, b)$  est une permutation impaire de  $E$ .

$$\text{Donc : } S(E) \not\subset A(E) = \{A(E), \tau A(E)\} \Rightarrow [S(E) : A(E)] = |S(E) \not\subset A(E)| = 2.$$

$$n! = |S(E)| = [S(E) : A(E)]|A(E)| = 2|A(E)| \Rightarrow |A(E)| = \frac{n!}{2}.$$

Par suite on a :  $[S(E) : A(E)] = 2$  et  $|A(E)| = \frac{n!}{2}.$

## 4 - Anneaux et les corps :

### 4-1-Généralités :

**Définition 4-1-1 :**

Soit  $(A, +, \cdot)$  un ensemble muni de deux lois de composition internes  $+$  et  $\cdot$ .

On dit que  $(A, +, \cdot)$  est un anneau ou  $A$  est un anneau si on a les 3 propriétés suivantes :

- i)  $(A, +, \cdot)$  est un groupe abélien.
- ii) La multiplication de  $A$  est associative.
- iii) La multiplication de  $A$  est distributive par rapport à l'addition de  $A$ .

**Dans ce cas :**

- \* On note par  $A^*$  l'ensemble  $A^* = A - \{0_A\}$ .
- \* Si  $A = \{0_A\}$  (c'est à dire si  $A^* = \emptyset$ ) on dit  $A$  est nul.
- \* Si la multiplication de  $A$  est commutative on dit que  $(A, +, \cdot)$  est un anneau abélien ou commutative.
- \* On dit que  $A$  est intègre si :  $\forall a, b \in A : ab = 0_A \Rightarrow [a = 0_A \text{ ou } b = 0_A]$ .  
C'est à dire :  $A$  est intègre  $\Leftrightarrow A^*$  est stable pour la multiplication
- \* Si  $A$  admet un élément neutre pour la multiplication de  $A$  on dit que  $A$  est un anneau unitaire.
- \* Si  $A$  est un anneau unitaire alors l'élément neutre pour la multiplication de  $A$  est appelé l'unité de  $A$  et noté  $1_A$  ou  $1$ .
- \* Si  $A$  est un anneau unitaire alors les éléments inversibles de  $A$  sont appelés les unités de  $A$ .
- \* Si  $A$  est un anneau unitaire alors l'ensemble des unités de  $A$  est noté  $U(A)$ .
- \* Si  $A$  est un anneau unitaire et si  $U(A) = A^*$  on dit que  $A$  est un corps.
- \* Soient  $B$  un autre anneau  $f$  une application de  $A$  vers  $B$ .  
Si  $f$  est homomorphisme de  $(A, +)$  vers  $(B, +)$  et si  $f$  est un homomorphisme de  $(A, \cdot)$  vers  $(B, \cdot)$  on dit que  $f$  est homomorphisme d'anneaux de  $A$  vers  $B$ .  
- Si  $A$  et  $B$  sont unitaires et si  $f(1_A) = 1_B$  on dit que  $f$  est un homomorphisme d'anneaux unitaire de  $A$  vers  $B$ .  
- Si  $A$  et  $B$  sont des corps on dit que  $f$  est un homomorphisme de corps.

**Exemple 4-1-2 :**

- \*  $\mathbb{Z}$  est un anneau abélien unitaire et  $U(\mathbb{Z}) = \{-1, 1\} \neq \mathbb{Z}^*$ .  
Donc  $\mathbb{Z}$  n'est pas un corps.
- \*  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$  sont des corps abéliens.
- \* Si  $E$  est un ensemble quelconque alors  $(\mathcal{P}(E), \Delta, \cap)$  est un anneau abélien unitaire.  
 $0_{\mathcal{P}(E)} = \emptyset$ ,  $1_{\mathcal{P}(E)} = E$  et  $U(\mathcal{P}(E)) = \{E\}$ .
- \* Si  $A$  et  $B$  sont des anneaux alors  $A \times B$  est un anneau (de même pour abélien et de même pour unitaires).
- \* Si  $A_1, A_2, \dots, A_n$  sont des anneaux alors  $A_1 \times A_2 \times \dots \times A_n$  est un anneau (de même pour abélien et de même pour unitaires).
- \* Si  $E$  est un ensemble quelconque non vide et si  $A$  est un anneau alors  $A^E$  est un anneau (de même pour abélien et de même pour unitaire).

**4-2-Règles de calcul et propriétés :**

Soit  $A$  un anneau.

- 1)  $0_A$  est un élément absorbant pour la multiplication.

C'est à dire :  $\forall a \in A : a0_A = 0_Aa = 0_A$ .

$$2) \begin{cases} A \text{ est unitaire} \\ 1_A = 0_A \end{cases} \Leftrightarrow A = \{0_A\}.$$

$$3) \text{ La règle des signes : } \forall a, b \in A : \begin{cases} a(-b) = (-a)b = -ab \\ (-a)(-b) = ab \end{cases}.$$

- 4)  $\forall a, b, c \in A : \begin{cases} a(b - c) = ab - ac \\ (b - c)a = ba - ca \end{cases}.$
- 5)  $\forall a, b \in A \quad \text{et} \quad \forall k \in \mathbb{N} : (ka)b = a(kb) = k(ab).$
- 6)  $\forall a, b \in A \quad \text{et} \quad \forall k \in \mathbb{Z} : (ka)b = a(kb) = k(ab).$
- 7)  $\forall a, b \in A \quad \text{tq} : ab = ba \quad \text{et} \quad \forall n \in \mathbb{N} \quad \text{tq} : n \geq 2 : (a + b)^n = a^n + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + b^n.$
- 8) Si  $A$  est unitaire alors :
- $$\forall a, b \in A \quad \text{tq} : ab = ba \quad \text{et} \quad \forall n \in \mathbb{N} : (a + b)^n = \sum_{k=0}^n C_n^k a^{n-k} b^k.$$
- 9)  $A$  est intègre si et seulement si tous les éléments non nuls de  $A$  sont réguliers pour la multiplication de  $A$ .
- 10) Si  $A$  est unitaire alors tous les éléments inversibles de  $A$  sont réguliers pour la multiplication de  $A$ .  
C'est à dire, si  $A$  est unitaire alors tous les éléments de  $U(A)$  sont réguliers pour la multiplication de  $A$ .
- 11) Si  $A$  est un corps alors  $A$  est intègre.
- 12) Soit  $B$  un autre anneau et  $f$  est un homomorphisme d'anneaux de  $A$  vers  $B$ .  
Si  $A$  est un corps et si  $f$  est non nul alors il est injectif.

### Démonstration :

$$1) \forall a \in A : \begin{cases} a0_A + a0_A = a(0_A + 0_A) = a0_A = a0_A + 0_A \Rightarrow a0_A = 0_A \\ 0_A a + 0_A a = (0_A + 0_A)a = 0_A a = 0_A a + 0_A \Rightarrow 0_A a = 0_A \end{cases}.$$

Alors :  $a0_A = 0_A a = 0_A$ .

Alors  $0_A$  est un élément absorbant pour la multiplication.

2)  $\Rightarrow$  ) **Si  $A$  est unitaire et si  $1_A = 0_A$  :**

Alors :  $\forall a \in A : a = a1_A = a0_A = 0_A$ . Donc  $A = \{0_A\}$ .

$\Leftarrow$  ) **Si  $A = \{0_A\}$  :**

Alors :  $\forall a \in A : a = 0_A \Rightarrow a0_A = 0_A a = 0_A = a$ .

Donc :  $\begin{cases} A \text{ est unitaire} \\ 1_A = 0_A \end{cases}.$

3)  $\forall a, b \in A :$

$$\bullet \begin{cases} ab + a(-b) = a[b + (-b)] = a0_A = 0_A \Rightarrow a(-b) = -ab \\ ab + (-a)b = [a + (-a)]b = 0_A b = 0_A \Rightarrow (-a)b = -ab \end{cases}.$$

Par suite on a :  $a(-b) = (-a)b = -ab$ .

$$\bullet (-a)(-b) = -[(-a)b] = -(-ab) = ab..$$

4)  $\forall a, b, c \in A :$

$$\begin{cases} a(b - c) = a[b + (-c)] = ab + a(-c) = ab + (-ac) = ab - ac \\ (b - c)a = [b + (-c)]a = ba + (-c)a = ba + (-ca) = ba - ca \end{cases}.$$

5) Soient  $a$  et  $b$  deux éléments quelconques de  $A$ .

Montrons par récurrence que pour tout entier naturel  $k$ ,  $(ka)b = a(kb) = k(ab)$ .

- **Pour  $k = 0$  :**

$$\begin{cases} (ka)b = (0a)b = 0_A b = 0_A = 0(ab) = k(ab) \\ a(kb) = a(0b) = a0_A = 0_A = 0(ab) = k(ab) \end{cases} \Rightarrow (ka)b = a(kb) = k(ab).$$

- **Pour  $k - 1$  :**

Supposons que  $[(k-1)a]b = a[(k-1)b] = (k-1)(ab)$ .

- **Pour  $k$  :**

Montrons qu'alors  $(ka)b = a(kb) = k(ab)$ .

$$\begin{cases} (ka)b = [(k-1)a + a]b = [(k-1)a]b + ab = (k-1)(ab) + ab = k(ab) \\ a(kb) = a[(k-1)b + b] = a[(k-1)b] + ab = (k-1)(ab) + ab = k(ab) \end{cases}.$$

On a alors  $(ka)b = a(kb) = k(ab)$ .

Ce qui montre que :  $\forall a, b \in A$  et  $\forall k \in \mathbb{N}$  :  $(ka)b = a(kb) = k(ab)$ .

6) Soient  $a$  et  $b$  deux éléments quelconques de  $A$ .

$\forall k \in \mathbb{Z}$  :

- **Si  $k \geq 0$  :**

D'après 5), on a :  $(ka)b = a(kb) = k(ab)$ .

- **Si  $k \leq 0$  :**

D'après 5), on a :  $[(-k)a]b = a[(-k)b] = (-k)(ab)$  (car  $-k \in \mathbb{N}$ ).

Par suite on a :

$$\begin{cases} (ka)b = [-(-k)a]b = -[(-k)a]b = -[(-k)(ab)] = k(ab) \\ a(kb) = a[-(-k)b] = -[a(-k)b] = -[(-k)(ab)] = k(ab) \end{cases}.$$

Ce qui montre que :  $\forall a, b \in A$  et  $\forall k \in \mathbb{Z}$  :  $(ka)b = a(kb) = k(ab)$ .

7) Soient  $a$  et  $b$  deux éléments quelconques de  $A$ .

Montrons par récurrence que pour tout entier naturel  $n \geq 2$  on a :

$$(a+b)^n = a^n + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + b^n.$$

- **Pour  $n = 2$  :**

$$(a+b)^n = (a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2$$

$$= a^2 + 2ab + b^2 = a^2 + C_2^1 ab + b^2 = a^2 + \sum_{k=1}^1 C_2^k a^1 b^1 + b^2$$

$$= a^2 + \sum_{k=1}^{2-1} C_2^k a^{2-1} b^k + b^2$$

$$= a^n + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + b^n.$$

- **Pour  $n - 1$  :**

$$\text{Supposons que : } (a+b)^{n-1} = a^{n-1} + \sum_{k=1}^{n-2} C_{n-1}^k a^{n-1-k} b^k + b^{n-1}.$$



- Pour n :

Montrons qu'alors :  $(a + b)^n = a^n + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + b^n$ .

$$\begin{aligned} (a + b)^n &= (a + b)^{n-1}(a + b) = \left[ a^{n-1} + \sum_{h=1}^{n-2} C_{n-1}^h a^{n-1-h} b^h + b^{n-1} \right] (a + b) \\ &= a^n + \sum_{h=1}^{n-2} C_{n-1}^h a^{n-1-h} b^h a + b^{n-1} a + a^{n-1} b + \sum_{h=1}^{n-2} C_{n-1}^h a^{n-1-h} b^h b + b^n \\ &= a^n + \sum_{h=1}^{n-2} C_{n-1}^h a^{n-h} b^h + ab^{n-1} + a^{n-1} b + \sum_{h=1}^{n-2} C_{n-1}^h a^{n-1-h} b^{h+1} + b^n. \end{aligned}$$

Posons :  $h + 1 = k$  alors :  $\sum_{h=1}^{n-2} C_{n-1}^h a^{n-1-h} b^{h+1} = \sum_{k=2}^{n-1} C_{n-1}^{k-1} a^{n-k} b^k$ .

Par suite on a :

$$\begin{aligned} (a + b)^n &= a^n + \sum_{k=1}^{n-2} C_{n-1}^k a^{n-k} b^k + a^{n-1} b + ab^{n-1} + \sum_{k=2}^{n-1} C_{n-1}^{k-1} a^{n-k} b^k + b^n \\ &= a^n + C_{n-1}^1 a^{n-1} b + \sum_{k=2}^{n-2} C_{n-1}^k a^{n-k} b^k + a^{n-1} b + ab^{n-1} \\ &\quad + \sum_{k=2}^{n-2} C_{n-1}^{k-1} a^{n-k} b^k + C_{n-1}^{n-1} ab^{n-1} + b^n \\ &= a^n + (n-1)a^{n-1} b + a^{n-1} b + \sum_{k=2}^{n-2} \left( C_{n-1}^k a^{n-k} b^k + C_{n-1}^{k-1} a^{n-k} b^k \right) \\ &\quad + (n-1)ab^{n-1} + b^n \\ &= a^n + na^{n-1} b + \sum_{k=2}^{n-2} \left( C_{n-1}^k + C_{n-1}^{k-1} \right) a^{n-k} b^k + na^{n-1} b + b^n \\ &= a^n + C_n^1 a^{n-1} b + \sum_{k=2}^{n-2} C_n^k a^{n-k} b^k + C_n^{n-1} a^{n-1} b + b^n \\ &= a^n + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + b^n. \end{aligned}$$

8) Supposons que A est unitaire.

$\forall a, b \in A \quad tq : ab = ba \quad et \quad \forall n \in \mathbb{N} :$

$$\begin{aligned} (a + b)^n &= a^n + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + b^n = a^n b^0 + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + a^0 b^n \\ &= C_n^0 a^n b^0 + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + C_n^n a^0 b^n \\ &= C_n^0 a^{n-0} b^0 + \sum_{k=1}^{n-1} C_n^k a^{n-k} b^k + C_n^n a^0 b^{n-0} \\ &= \sum_{k=0}^n C_n^k a^{n-k} b^k. \end{aligned}$$

9)  $\Rightarrow$  ) **Si A est intègre :**

Soit  $a$  un élément non nul quelconque de  $A$ .

$\forall x, y \in A :$

$$\begin{cases} ax = ay \Rightarrow ax - ay = 0_A \Rightarrow a(x - y) = 0_A \Rightarrow x - y = 0_A \Rightarrow x = y \\ xa = ya \Rightarrow xa - ya = 0_A \Rightarrow (x - y)a = 0_A \Rightarrow x - y = 0_A \Rightarrow x = y \end{cases}$$

Alors  $a$  est régulier pour la multiplication de  $A$ .

Ce qui montre que tous les éléments non nuls de  $A$  sont réguliers pour la multiplication de  $A$ .

$\Leftarrow$  ) **Si tous les éléments non nuls de A sont réguliers pour la multiplication de A :**

Supposons  $A$  n'est pas intègre.

Alors il existe deux éléments non nuls  $a$  et  $b$  de  $A$  tels que le produit  $ab$  est nul.  $ab$  est nul.

Puisque  $a$  est non nul alors  $a$  est régulier pour la multiplication de  $A$ .

$ab = 0_A \Rightarrow b = 0_A$ . Ce qui est absurde.

Donc  $A$  est intègre.

10) Supposons que  $A$  est unitaire.

$\forall a \in U(A)$  et  $\forall x, y \in A :$

$$\begin{cases} ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow (a^{-1}a)x = (a^{-1}a)y \Rightarrow 1_A x = 1_A y \Rightarrow x = y \\ xa = ya \Rightarrow (xa)a^{-1} = (ya)a^{-1} \Rightarrow x(aa^{-1}) = y(aa^{-1}) \Rightarrow x1_A = y1_A \Rightarrow x = y \end{cases}$$

Donc  $a$  est régulier pour la multiplication de  $A$ .

Ce qui montre que tous les éléments inversibles de  $A$  sont réguliers pour la multiplication de  $A$ .

11) Supposons que  $A$  est un corps.

$\forall a \in A^* : a \in U(A)$  (car  $U(A) = A^*$ ).

Donc  $a$  est régulier pour la multiplication de  $A$ .

Ce qui montre que  $A$  est intègre.

12) Soit  $B$  un autre anneau et  $f$  est un homomorphisme d'anneaux de  $A$  vers  $B$ .

Supposons que  $A$  est un corps et que  $f$  est non nul.

Supposons que  $f$  n'est pas injectif.

Alors :  $\ker f \neq \{0_A\} \Rightarrow \exists a \in A^* = U(A)$  (car  $A$  est un corps) tel que :  $f(a) = 0_B$

$\forall x \in A : f(x) = f(aa^{-1}x) = f(a)f(a^{-1}x) = 0_B f(a^{-1}x) = 0_B$

Donc  $f$  est nul. Ce qui est absurde.

Ce qui montre que  $f$  est injectif.

#### 4-3-Sous-anneaux et sous-corps :

##### Définition 4-3-1 :

Soient  $A$  un anneau et  $B$  une partie de  $A$ .

- On dit que  $B$  est un sous-anneau de  $A$  ou  $A$  est sur-anneau de  $B$  si on a les 3 propriétés suivantes :

i)  $B$  est stable pour l'addition de  $A$ .

ii)  $B$  est stable pour la multiplication de  $A$ .

iii)  $B$  est un anneau pour les restrictions des deux lois de  $A$ .

- On dit que  $B$  est un sous-corps de  $A$  si  $B$  est un sous-anneau de  $A$  et si  $(B, +, \cdot)$  est un corps.

**Théorème 4-3-2 :**

Soient  $A$  un anneau et  $B$  une partie de  $A$ .

Pour que  $B$  soit un sous anneau de  $A$  il faut et il suffit qu'on a les deux propriétés suivantes :

- i)  $B$  est sous groupe de  $(A, +)$ .
- ii)  $B$  est stable pour la multiplication de  $A$ .

**Exemples 4-3-3 :**

- \* Les sous-anneaux de  $\mathbb{Z}$  sont les parties de  $\mathbb{Z}$  de la forme  $n\mathbb{Z}$  telle que  $n \in \mathbb{N}$ .
- \*  $\mathbb{Z}$  est un sous-anneaux de  $\mathbb{Q}$ , de  $\mathbb{R}$  et de  $\mathbb{C}$ .
- \*  $\mathbb{Q}$  est un sous-corps de  $\mathbb{R}$  et de  $\mathbb{C}$ .
- \*  $\mathbb{R}$  est un sous-corps de  $\mathbb{C}$ .

**Propriétés 4-3-4 :**

Soit  $A$  un anneau.

- 1)  $A$  et  $\{0_A\}$  sont des sous-anneaux de  $A$  appelés les sous-anneaux triviaux de  $A$ .  
 $\{0_A\}$  est appelé le sous-anneau nul de  $A$ .
- 2) Soit  $A'$  un autre anneau et  $f$  est un homomorphisme d'anneaux de  $A$  vers  $A'$ .
  - i) Si  $B$  est un sous-anneau de  $A$  alors  $f(B)$  est un sous-anneau de  $A'$ .
  - ii) Si  $B'$  est un sous-anneau de  $A'$  alors  $f^{-1}(B')$  est un sous-anneau de  $A$ .
  - iii)  $\ker f$  est un sous-anneau de  $A$ .
- 3) Si  $B$  et  $C$  sont des sous-anneaux de  $A$  alors  $B \cap C$  est aussi un sous-anneau de  $A$ .
- 4) Si  $\mathcal{M}$  est un ensemble non vide de sous-anneaux de  $A$  alors  $\bigcap_{M \in \mathcal{M}} M$  est un sous-anneau de  $A$ .
- 5) Si  $I$  est un ensemble non vide et si  $(M_i)_{i \in I}$  est une famille de sous-anneaux de  $A$  alors  $\bigcap_{i \in I} M_i$  est un sous-anneau de  $A$ .
- 6) Si  $A$  est unitaire et si  $B$  est un sous anneau unitaire de  $A$  alors en général on a :  
 $1_B \neq 1_A$ .
- 7) Soit  $B$  un sous anneau quelconque de  $A$ .  
 Si  $A$  est unitaire et si  $1_A \in B$  alors  $B$  est unitaire et  $1_B = 1_A$ .
- 8) Si  $A$  est unitaire intègre alors tous les sous anneaux unitaires nonnuls de  $A$  ont le même unité que ce lui de  $A$ .

**Démonstration :**

- 1) • Puisque  $A$  est une partie de  $A$  et puisque  $A$  est un anneau, alors  $A$  est un sous-anneau de  $A$ .
  - $\star \{0_A\}$  est un sous-groupe de  $(A, +)$ .  
 $\star \forall a, b \in \{0_A\} : a = b = 0_A \Rightarrow ab = 0_A 0_A = 0_A \in \{0_A\}$ .  
 Donc  $\{0_A\}$  est stable pour la multiplication de  $A$ .  
 Ce qui montre que  $\{0_A\}$  est un sous-anneau de  $A$ .
- 2) i) Supposons que  $B$  est un sous-anneau de  $A$ .
  - $f(B)$  est un sous-groupe de  $(A', +)$  (car  $B$  est un sous-groupe de  $(A, +)$ ).
  - $\forall x, y \in f(B) : \exists a, b \in B \text{ tq } : x = f(a) \text{ et } y = f(b)$ .  
 Alors :  $xy = f(a)f(b) = f(ab) \in f(B)$ .  
 Donc  $f(B)$  est stable pour la multiplication de  $A'$ .  
 Ce qui montre que  $f(B)$  est un sous-anneau de  $A'$ .

ii) Supposons que  $B'$  est un sous-anneau de  $A'$ .

- $f^{-1}(B')$  est un sous-groupe de  $(A, +)$  (car  $B'$  est un sous-groupe de  $(A', +)$ ).
- $\forall a, b \in f^{-1}(B') : f(a), f(b) \in B'$ .

$$\text{Alors : } f(ab) = f(a)f(b) \in B' \Rightarrow ab \in f^{-1}(B').$$

Donc  $f^{-1}(B')$  est stable pour la multiplication de  $A$ .

Ce qui montre que  $f^{-1}(B')$  est un sous-anneau de  $A$ .

iii) Puisque  $\{0_{A'}\}$  est un sous-anneau de  $A'$  alors (d'après ii)),  $\ker f = f^{-1}(\{0_{A'}\})$  est un sous-anneau de  $A$ .

3) Soient  $B$  et  $C$  deux sous-anneaux de  $A$ .

- $B \cap C$  est un sous-groupe de  $(A, +)$  (car  $B$  et  $C$  sont des sous-groupes de  $(A, +)$ ).
- $\forall a, b \in B \cap C : [a, b \in B \text{ et } a, b \in C] \Rightarrow [ab \in B \text{ et } ab \in C] \Rightarrow ab \in B \cap C$ .

Donc  $B \cap C$  est stable pour la multiplication de  $A$ .

Ce qui montre que  $B \cap C$  est un sous-anneau de  $A$ .

4) Supposons que  $\mathcal{M}$  est un ensemble non vide de sous-anneaux de  $A$ .

- $\bigcap_{M \in \mathcal{M}} M$  est un sous-groupe de  $(A, +)$  (car  $M$  est un sous-groupe de  $(A, +)$  pour tout élément  $M$  de  $\mathcal{M}$ ).

- $\forall a, b \in \bigcap_{M \in \mathcal{M}} M : [\forall M \in \mathcal{M} : a, b \in M] \Rightarrow [\forall M \in \mathcal{M} : ab \in M]$

$$\Rightarrow ab \in \bigcap_{M \in \mathcal{M}} M.$$

Donc  $\bigcap_{M \in \mathcal{M}} M$  est stable pour la multiplication de  $A$ .

Ce qui montre que  $\bigcap_{M \in \mathcal{M}} M$  est un sous-anneau de  $A$ .

5) Supposons que  $I$  est un ensemble non vide et que  $(M_i)_{i \in I}$  est une famille de sous-anneaux de  $A$ .

- $\bigcap_{i \in I} M_i$  est un sous-groupe de  $(A, +)$  (car  $M_i$  est un sous-groupe de  $(A, +)$  pour tout élément  $i$  de  $I$ ).

- $\forall a, b \in \bigcap_{i \in I} M_i : [\forall i \in I : a, b \in M_i] \Rightarrow [\forall i \in I : a, b \in M_i]$

$$\Rightarrow ab \in \bigcap_{i \in I} M_i.$$

Donc  $\bigcap_{i \in I} M_i$  est stable pour la multiplication de  $A$ .

Ce qui montre que  $\bigcap_{i \in I} M_i$  est un sous-anneau de  $A$ .

6) **Contre exemple :**

Pour  $A = \mathbb{Z} \times \mathbb{Z}$ , qui est un anneau unitaire et  $B = \mathbb{Z} \times \{0\}$ , qui est un sous-anneau unitaire de  $A$  on a :  $1_B = (1, 0) \neq (1, 1) = 1_A$ .

7) Supposons que  $A$  est unitaire et que  $1_A \in B$ .

Alors :  $1_A \in B$  et  $\forall a \in B : a1_A = 1_A = a$ .

Donc  $B$  est unitaire et  $1_B = 1_A$ .

8) Supposons que  $A$  est unitaire intègre.

Soit  $B$  un sous-anneau unitaire non nul quelconque de  $A$ .

$$B \neq \{0_B\} \Rightarrow 1_B \neq 0_B = 0_A.$$

Alors  $1_B$  est régulier pour la multiplication de  $A$  (car  $A$  est intègre).

$$\text{Donc : } 1_B 1_B = 1_B = 1_B 1_A \Rightarrow 1_B = 1_A.$$

Ce qui montre que les sous anneaux unitaires non nuls de  $A$  ont le même unité que ce lui de  $A$ .

#### 4-4-Fractions et corps de fractions :

##### Notation 4-4-1 :

Soient  $A$  un anneau unitaire et  $a, b \in A$ .

Si  $b \in U(A)$  et si  $a$  et  $b$  commutent alors  $ab^{-1}$  est noté aussi  $\frac{a}{b}$ .

$\frac{a}{b} = ab^{-1}$  est appelé la fraction  $a$  sur  $b$ .

##### Propriétés 4-4-2 :

Soient  $A$  un anneau unitaire et  $a, b, c, d \in A$  qui commutent.

- 1)  $\frac{a}{1} = a$ .
- 2) Si  $b \in U(A)$  alors :  $\frac{a}{b} = 0 \Leftrightarrow a = 0$ .
- 3) Si  $b \in U(A)$  alors :  $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$ .
- 4) Si  $b \in U(A)$  alors :  $\forall k \in \mathbb{Z} : k\left(\frac{a}{b}\right) = \frac{ka}{b}$ .
- 5) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :  $\frac{ad}{bd} = \frac{a}{b}$ .
- 6) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :  $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ .
- 7) Si  $d \in U(A)$  alors :  $\frac{a}{d} + \frac{b}{d} = \frac{a+b}{d}$ .
- 8) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ .
- 9) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :  $\frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$ .
- 10) Si  $a \in U(A)$  et si  $b \in U(A)$  alors :  $\left(\frac{a}{b}\right)^{-1} = \frac{1}{\frac{a}{b}} = \frac{b}{a}$ .
- 11) Si  $b \in U(A)$ ,  $c \in U(A)$  et  $d \in U(A)$  alors :  $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \frac{d}{c} = \frac{ad}{bc}$ .

##### Démonstration :

$$1) \frac{a}{1} = a1^{-1} = a1 = a.$$

2) Si  $b \in U(A)$  alors :

$$\frac{a}{b} = 0 \Leftrightarrow ab^{-1} = 0 \Leftrightarrow (ab^{-1})b = 0b \text{ (car } b \text{ est régulier pour la multiplication de } A).$$

$$\Leftrightarrow a(b^{-1}b) = 0 \Leftrightarrow a1 = 0$$

$$\Leftrightarrow a = 0.$$

3) Si  $b \in U(A)$  alors :

$$\begin{cases} -\frac{a}{b} = -(ab^{-1}) = (-a)b^{-1} = \frac{-a}{b} \\ \frac{-a}{b} = \frac{(-a)(-1)}{b(-1)} = \frac{a1}{-(b1)} = \frac{a}{-b} \end{cases} \Rightarrow -\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}.$$

$$4) \text{ Si } b \in U(A) \text{ alors : } \forall k \in \mathbb{Z} : k\left(\frac{a}{b}\right) = k(ab^{-1}) = (ka)b^{-1} = \frac{ka}{b}.$$

5) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :

$$\frac{ad}{bd} = ad(bd)^{-1} = ad(d^{-1}b^{-1}) = a(dd^{-1})b^{-1} = a1b^{-1} = ab^{-1} = \frac{a}{b}.$$

6) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ab^{-1} = cd^{-1}$$

$$\Leftrightarrow (ab^{-1})(bd) = (cd^{-1})(bd) \text{ (car } bd \text{ est régulier pour la multiplication de } A).$$

$$\Leftrightarrow a(b^{-1}b)d = c(d^{-1}b)d \Leftrightarrow a1d = c1d$$

$$\Leftrightarrow ad = bc.$$

7) Si  $d \in U(A)$  alors :  $\frac{a}{d} + \frac{b}{d} = ad^{-1} + bd^{-1} = (a+b)d^{-1} = \frac{a+b}{d}.$

8) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :  $\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{cb}{db} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}.$

9) Si  $b \in U(A)$  et si  $d \in U(A)$  alors :

$$\begin{aligned} \frac{a}{b} \frac{c}{d} &= (ab^{-1})(cd^{-1}) = a(b^{-1}c)d^{-1} = a(cb^{-1})d^{-1} = (ac)(b^{-1}d^{-1}) = (ac)(d^{-1}b^{-1}) \\ &= (ac)(bd)^{-1} \\ &= \frac{ac}{bd}. \end{aligned}$$

10) Si  $a \in U(A)$  et si  $b \in U(A)$  alors :

$$\bullet \left(\frac{a}{b}\right)^{-1} = 1\left(\frac{a}{b}\right)^{-1} = \frac{1}{\frac{a}{b}}.$$

$$\bullet \left(\frac{a}{b}\right)^{-1} = (ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1} = \frac{b}{a}.$$

$$\text{Par suite on a : } \left(\frac{a}{b}\right)^{-1} = \frac{1}{\frac{a}{b}} = \frac{b}{a}.$$

11) Si  $b \in U(A)$ ,  $c \in U(A)$  et  $d \in U(A)$  alors :

$$\bullet \frac{\frac{a}{b}}{\frac{c}{d}} = \left(\frac{a}{b}\right)\left(\frac{c}{d}\right)^{-1} = \frac{a}{b} \frac{d}{c}.$$

$$\bullet \frac{a}{b} \frac{d}{c} = \frac{ad}{bc} \text{ (d'après 7)).}$$

$$\text{Par suite on a : } \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \frac{d}{c} = \frac{ad}{bc}.$$

### **Théorème et définition 4-4-3 :**

Si  $E$  est un corps et si  $A$  est un sous-anneau commutatif non nul de  $E$  alors

l'ensemble  $K = \left\{ \frac{a}{b} \mid a, b \in A \text{ et } b \neq 0 \right\}$  est un sous-corps commutatif de  $E$

et c'est le plus petit sous-corps de  $E$  contenant  $A$ .

$K$  est appelé le corps des fractions de  $A$  dans  $E$ .

On dit aussi que  $K$  est un corps des fractions de  $A$ .

### **Démonstration :**

Supposons que  $E$  est un corps et que  $A$  est un sous-anneau commutatif non nul de  $E$ .

Montrons que l'ensemble  $K = \left\{ \frac{a}{b} \mid a, b \in A \text{ et } b \neq 0 \right\}$  est un sous-corps commutatif de  $E$  contenant  $A$  et c'est le plus petit sous-corps de  $E$  contenant  $A$ .

• Montrons que l'ensemble  $K$  est un sous-corps commutatif de  $E$  contenant  $A$ .

★ Soit  $u$  un élément non nul de  $A$  ( $u$  existe car  $A$  est un non nul).

$$\forall a \in A : a = \frac{a}{1} = \frac{au}{1u} = \frac{au}{u} \in K. \text{ Donc : } A \subset K.$$

★ –  $[A \neq \emptyset \text{ et } A \subset K] \Rightarrow K \neq \emptyset.$

–  $\forall x, y \in K : \exists a, b, c, d \in A \text{ tq : } b \neq 0, c \neq 0, x = \frac{a}{b} \text{ et } y = \frac{c}{d}.$   
 $x - y = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in K.$

Donc  $K$  est un sous-groupe de  $(E, +).$

★ –  $\forall x, y \in K : \exists a, b, c, d \in A \text{ tq : } b \neq 0, c \neq 0, x = \frac{a}{b} \text{ et } y = \frac{c}{d}.$   
 $xy = \frac{a}{b} \frac{c}{d} = \frac{ac}{bd} \in K.$

Donc  $K$  est une partie stable de  $E$  pour la multiplication de  $E.$

–  $\forall x, y \in K : \exists a, b, c, d \in A \text{ tq : } b \neq 0, c \neq 0, x = \frac{a}{b} \text{ et } y = \frac{c}{d}.$   
 $xy = \frac{a}{b} \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \frac{a}{b} = yx.$

Donc la restriction de la multiplication de  $E$  dans  $K$  est commutative.

Par suite  $K$  est un sous-anneau commutatif de  $E.$

★ Soit  $u$  un élément non nul de  $A$  ( $u$  existe car  $A$  est un non nul).

$$1 = \frac{u}{u} \in K.$$

Donc  $K$  est un sous-anneau commutatif unitaire non nul de  $E.$

★ –  $K^* \neq \emptyset \Rightarrow U(K) \subset K^*.$

–  $\forall x \in K^* : \exists a, b \in A \text{ tq : } b \neq 0 \text{ et } x = \frac{a}{b}. \frac{a}{b} \neq 0 \Rightarrow a \neq 0.$

$$\text{Alors : } x^{-1} = \left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \in K^* \Rightarrow x \in U(K).$$

Donc  $U(K) \subset K^*.$  Par suite  $K$  est un corps commutatif.

Ce qui montre que  $K$  est un sous-corps commutatif de  $E$  contenant  $A.$

• Montrons que  $K$  est le plus petit sous-corps de  $E$  contenant  $A.$

Soit  $M$  un sous-corps quelconque de  $E$  contenant  $A.$

$\forall x \in K : \exists a, b \in A \text{ tq : } b \neq 0 \text{ et } x = \frac{a}{b} = ab^{-1}.$

$$a, b \in A \subset M \Rightarrow ab^{-1} \in M \Rightarrow x = ab^{-1} \in M.$$

Alors  $K \subset M.$

Ce qui prouve que  $K$  est le plus petit sous-corps de  $E$  contenant  $A.$

#### Exemple 4-4-4 :

★  $\mathbb{Q}$  est le corps des fractions de  $\mathbb{Z}$  dans  $\mathbb{Q}$ , dans  $\mathbb{R}$  et dans  $\mathbb{C}.$

★ Pour tout entier naturel non nul  $n$ ,  $\mathbb{Q}$  est le corps des fractions de  $n\mathbb{Z}$  dans  $\mathbb{Q}$ , dans  $\mathbb{R}$  et dans  $\mathbb{C}.$

#### Théorème 4-4-5 :

Soit  $A$  un anneau commutatif intègre non nul et  $u$  un élément quelconque de  $A^*.$

On munit  $A \times A^*$  de :

– la multiplication suivant :  $\forall x = (a, b) \in A \times A^* \text{ et } \forall y = (c, d) \in A \times A^* :$   
 $xy = (a, b)(c, d) = (ac, bd).$

– la relation  $R_A$  définie par :  $\forall x = (a, b) \in A \times A^* \text{ et } \forall y = (c, d) \in A \times A^* :$   
 $xR_A y \Leftrightarrow (a, b)R_A(c, d) \Leftrightarrow ad = bc.$

Les propriétés suivantes sont vérifiées :

- 1) La multiplication de  $A \times A^*$  est commutative et associative.
- 2)  $R_A$  est une relation d'équivalence dans l'ensemble  $A \times A^*.$

- 3)  $\overline{(0_A, u)} = \{(0_A, b) \mid b \in A^*\}$  où  $\overline{(0_A, u)}$  est la classe de  $(0_A, u)$  pour la relation d'équivalence  $R_A$ .
- 4)  $\overline{(u, u)} = \{(b, b) \mid b \in A^*\}$  où  $\overline{(u, u)}$  est la classe de  $(u, u)$  pour la relation d'équivalence  $R_A$ .
- 5) Il existe une multiplication dans l'ensemble  $K = (A \times A^*)/R_A$  et une seule telle que la surjection canonique  $p$  de  $A \times A^*$  vers  $(A \times A^*)/R_A$  soit un homomorphisme de  $(A \times A^*, \cdot)$  vers  $(K, \cdot)$ .
- 6) La multiplication de  $K$  est commutative et associative.
- 7)  $\overline{(u, u)}$  est l'élément neutre de  $K$  pour la multiplication.
- 8) Si  $(a, b)$  est un élément quelconque de  $A \times A^*$  alors  $\overline{(a, b)}$  est inversible si et seulement si  $a \neq 0_A$ , et dans ce cas :  $\overline{(a, b)}^{-1} = \overline{(b, a)}$ .
- 9) Si  $x$  et  $y$  sont des éléments quelconques de  $K$ , il existe des éléments  $a, b, d \in A$  tels que :  $d \neq 0_A$ ,  $x = \overline{(a, d)}$  et  $y = \overline{(b, d)}$ .
- 10) Pour tout entier naturel  $n \geq 2$ , si  $x_1, \dots, x_n$  sont des éléments quelconques de  $K$ , il existe des éléments  $a_1, \dots, a_n, d \in A$  tels que :  $d \neq 0_A$  et  $\forall i = 1, \dots, n : x_i = \overline{(a_i, d)}$ .
- 11) Il existe une addition dans l'ensemble  $K = (A \times A^*)/R_A$  et une seule telle que :  $\forall a, b \in A$  et  $\forall d \in A^* : \overline{(a, d)} + \overline{(b, d)} = \overline{(a + b, d)}$ .
- 12) L'addition de  $K$  est commutative et associative.
- 13) La multiplication de  $K$  est distributive par rapport à l'addition.
- 14)  $\overline{(0_A, u)}$  est le zéro de  $K$ .
- 15) Si  $(a, b)$  est un élément quelconque de  $A \times A^*$  alors  $\overline{(a, b)}$  admet un opposé et on a :  $-\overline{(a, b)} = \overline{(-a, b)}$ .
- 16)  $K$  est un corps commutatif.
- 17) L'application suivante :  $\varphi : A \rightarrow K$   

$$a \mapsto \varphi(a) = \overline{(au, u)}$$
est un homomorphisme injectif de  $(A, +, \cdot)$  vers  $(K, +, \cdot)$ .  
Par la suite on confond chaque élément  $a$  de  $A$  avec  $\varphi(a)$ .
- 18)  $A$  est un sous-anneau de  $K$ .
- 19)  $\forall (a, b) \in A \times A^* : \overline{(a, b)} = \frac{a}{b}$ .
- 20)  $K$  est un corps des fractions de  $A$ .

### Démonstration :

- 1) •  $\forall x = (a, b) \in A \times A^*$  et  $\forall y = (c, d) \in A \times A^* :$   

$$xy = (a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b) = yx.$$
Alors la multiplication de  $A \times A^*$  est commutative.
  - $\forall x = (a, b) \in A \times A^*, \forall y = (c, d) \in A \times A^*$  et  $\forall z = (e, f) \in A \times A^* :$   

$$\begin{aligned} (xy)z &= [(a, b)(c, d)](e, f) = (ac, bd)(e, f) = ((ac)e, (bd)f) = (a(ce), b(df)) \\ &= (a, b)(ce, df) = (a, b)[(c, d)(e, f)] \\ &= x(yz). \end{aligned}$$
Alors la multiplication de  $A \times A^*$  est associative.
- Ce qui montre que la multiplication de  $A \times A^*$  est commutative et associative.



- 2) •  $\forall x = (a, b) \in A \times A^* : ab = ba \Rightarrow (a, b)R_A(a, b) \Rightarrow xR_{AX}$ .

Alors la relation  $R_A$  est une réflexive dans l'ensemble  $A \times A^*$ .

- $\forall x = (a, b) \in A \times A^* \quad \text{et} \quad \forall y = (c, d) \in A \times A^* :$   
 $xR_{AY} \Rightarrow (a, b)R_A(c, d) \Rightarrow ad = bc \Rightarrow bc = ad \Rightarrow cb = da \Rightarrow (c, d)R_A(a, b)$   
 $\Rightarrow yR_{AX}$ .

Alors la relation  $R_A$  est une symétrique dans l'ensemble  $A \times A^*$ .

- $\forall x = (a, b) \in A \times A^*, \quad \forall y = (c, d) \in A \times A^* \quad \text{et} \quad \forall z = (e, f) \in A \times A^* :$   

$$\begin{cases} xR_{AY} \\ yR_{AZ} \end{cases} \Rightarrow \begin{cases} (a, b)R_A(c, d) \\ (c, d)R_A(e, f) \end{cases} \Rightarrow \begin{cases} ad = bc \\ cf = de \end{cases} \Rightarrow \begin{cases} adf = bcf \\ bcf = bde \end{cases} \Rightarrow adf = bde$$
  
 $\Rightarrow (af)d = (be)d \Rightarrow af = be \Rightarrow (a, b)R_A(e, f)$   
 $\Rightarrow xR_{AZ}$ .

Alors la relation  $R_A$  est une transitive dans l'ensemble  $A \times A^*$ .

Ce qui montre que  $R_A$  est une relation d'équivalence dans l'ensemble  $A \times A^*$ .

- 3)  $\forall (a, b) \in A \times A^* : (a, b) \in \overline{(0_A, u)} \Leftrightarrow au = b0_A = 0_A \Leftrightarrow a = 0_A \text{ (car } u \neq 0_A \text{)}.$

Donc  $\overline{(0_A, u)} = \{(0_A, b) \mid b \in A^*\}$

- 4)  $\forall (a, b) \in A \times A^* : (a, b) \in \overline{(u, u)} \Leftrightarrow au = bu \Leftrightarrow a = b \text{ (car } u \neq 0_A \text{)}.$

Donc  $\overline{(u, u)} = \{(b, b) \mid b \in A^*\}$

- 5) • Soit  $f$  la relation de  $K \times K$  vers  $K$  définie par :

$$\forall x, y, z \in K : (x, y)fz \Leftrightarrow \exists s \in x \quad \text{et} \quad \exists t \in y \text{ tq : } st \in z.$$

Montrons que  $f$  est une loi de composition interne dans  $K$  qui sera noté multiplicativement.

$$- \forall x, y, z, z' \in K \text{ tq : } [(x, y)fz \text{ et } (x, y)fz'], \begin{cases} \exists s \in x \text{ et } \exists t \in y \text{ tq : } st \in z \\ \exists s' \in x \text{ et } \exists t' \in y \text{ tq : } s't' \in z' \end{cases}.$$

$$\exists (a, b), (a', b'), (c, d), (c', d') \in A \times A^* \text{ tq : } \begin{cases} s = (a, b) \text{ et } s' = (a', b') \\ t = (c, d) \text{ et } t' = (c', d') \end{cases}.$$

$$(a, b), (a', b') \in x \Rightarrow (a, b)R_A(a', b') \Rightarrow ab' = ba'.$$

$$(c, d), (c', d') \in y \Rightarrow (c, d)R_A(c', d') \Rightarrow cd' = dc'.$$

$$(ac)(b'd') = acb'd' = ab'cd' = (ab')(cd') = (ba')(dc') = ba'dc' = bda'c' = (bd)(a'c').$$

Alors :

$$(ac, bd)R_A(a'c', b'd') \Rightarrow (a, b)(c, d)R_A(a', b')(c', d') \Rightarrow stR_{As't'} \Rightarrow \overline{st} = \overline{s't'} \Rightarrow z = z'.$$

Donc  $f$  est une fonction de  $K \times K$  vers  $K$ .

$$- \forall (x, y) \in K \times K : \exists s, t \in A \times A^* \text{ tq : } x = \bar{s} \quad \text{et} \quad y = \bar{t}.$$

$$\text{Posons } z = \overline{st}. \begin{cases} s \in \bar{s} = x \\ t \in \bar{t} = y \Rightarrow (x, y)fz \Rightarrow (x, y) \in D_f. \\ st \in z \end{cases}$$

Donc  $D_f = K \times K$ . Par suite  $f$  est une application de  $K \times K$  vers  $K$ .

Ce qui montre que  $f$  est une loi de composition interne dans  $K$ .

La loi  $f$  est notée multiplicativement.

- Montrons que la surjection canonique  $p$  de  $A \times A^*$  vers  $(A \times A^*)/R_A$  est un homomorphisme de  $(A \times A^*, \cdot)$  vers  $(K, \cdot)$ .

$\forall s, t \in A \times A^*$  :

$$\text{Posons } z = \overline{st}, \quad \begin{cases} s \in \bar{s} \\ t \in \bar{t} \\ st \in \overline{st} = z \end{cases} \Rightarrow (\bar{s}, \bar{t})fz \Rightarrow z = f((\bar{s}, \bar{t})) \Rightarrow \overline{st} = \overline{st} \Rightarrow p(st) = p(s)p(t).$$

Donc  $p$  est un homomorphisme de  $(A \times A^*, \cdot)$  vers  $(K, \cdot)$ .

- Soit  $\times$  une loi de composition interne quelconque dans  $K$  telle que  $p$  soit un homomorphisme de  $(A \times A^*, \cdot)$  vers  $(K, \times)$ .

$$\forall x, y \in K : \exists s, t \in A \times A^* \text{ tq : } x = p(s) \quad \text{et} \quad y = p(t).$$

$$x \times y = p(s) \times p(t) = p(st) = p(s)p(t) = xy.$$

Ce qui montre qu'il existe une multiplication dans l'ensemble  $K = A \times A^*/R_A$  et une seule telle que la surjection canonique  $p$  de  $A \times A^*$  vers  $A \times A^*/R_A$  soit un homomorphisme de  $(A \times A^*, \cdot)$  vers  $(K, \cdot)$ .

- 6) •  $\forall x, y \in K : \exists s, t \in A \times A^* \text{ tq : } x = p(s) \quad \text{et} \quad y = p(t).$

$$xy = p(s)p(t) = p(st) = p(ts) = p(t)p(s) = yx.$$

Alors la multiplication de  $K$  est commutative.

- $\forall x, y, z \in K : \exists s, t, r \in A \times A^* \text{ tq : } x = p(s), \quad y = p(t) \quad \text{et} \quad z = p(r).$

$$(xy)z = [p(s)p(t)]p(r) = p(st)p(r) = p((st)r) = p(s(tr)) = p(s)p(tr) = p(s)[p(t)p(r)] = x(yz).$$

Alors la multiplication de  $K$  est associative.

Ce qui montre que la multiplication de  $K$  est commutative et associative.

- 7)  $\forall x \in K : \exists (a, b) \in A \times A^* \text{ tq : } x = p((a, b)) = \overline{(a, b)}.$

$$x(\overline{u, u}) = p((a, b))p((u, u)) = p((a, b)(u, u)) = p((au, bu)) = \overline{(au, bu)}.$$

$$(au)b = aub = bua = (bu)a \Rightarrow (au, bu)R_A(a, b) \Rightarrow \overline{(au, bu)} = \overline{(a, b)} = x.$$

$$\text{Alors : } x(\overline{u, u}) = \overline{(u, u)}x = x.$$

Donc  $\overline{(u, u)}$  est l'élément neutre de  $K$  pour la multiplication.

- 8) Soit  $(a, b)$  un élément quelconque de  $A \times A^*$ .

$\Rightarrow$  ) **Si  $\overline{(a, b)}$  est inversible :**

$$\exists (a', b') \in A \times A^* \text{ tq : } \overline{(a, b)}^{-1} = \overline{(a', b')}.$$

$$\text{Alors : } \overline{(aa', bb')} = \overline{(a, b)}\overline{(a', b')} = \overline{(a, b)}\overline{(a', b')} = \overline{(a, b)}\overline{(a, b)}^{-1} = \overline{(u, u)}.$$

$$\text{Donc : } (aa', bb') \in \overline{(u, u)} \Rightarrow aa' = bb' \neq 0_A \text{ (d'après 4))} \Rightarrow a \neq 0_A.$$

$\Leftarrow$  ) **Si  $a \neq 0_A$  :**

$$\text{Alors : } (b, a) \in A \times A^* \text{ et on a : } \overline{(a, b)}^{-1} = \overline{(b, a)}.$$

$$\overline{(a, b)}\overline{(b, a)} = \overline{(a, b)}\overline{(b, a)} = \overline{(ab, ba)} = \overline{(ab, ab)} = \overline{(u, u)} \text{ (d'après 4)).}$$

$$\text{Donc } \overline{(a, b)} \text{ est inversible et } \overline{(a, b)}^{-1} = \overline{(b, a)}.$$

Ce qui montre que  $\overline{(a, b)}$  est inversible si et seulement si  $a \neq 0_A$ , et dans ce cas  $\overline{(a, b)}^{-1} = \overline{(b, a)}$ .

- 9) Soient  $x$  et  $y$  deux éléments quelconques de  $K$ .

Il existe deux éléments  $(a_1, a_2), (b_1, b_2) \in A \times A^*$  tels que,  $x = \overline{(a_1, a_2)}$  et  $y = \overline{(b_1, b_2)}$ .

Puisque (d'après 4)),  $\overline{(u, u)} = \overline{(a_2, a_2)} = \overline{(b_2, b_2)}$  et puisque (d'après 7)),  $\overline{(u, u)} = \overline{(a_2, a_2)} = \overline{(b_2, b_2)}$  est l'élément neutre de  $(K, .)$  alors :

$$\begin{cases} x = x\overline{(b_2, b_2)} = \overline{(a_1, a_2)}\overline{(b_2, b_2)} = \overline{(a_1, a_2)(b_2, b_2)} = \overline{(a_1b_2, a_2b_2)} \\ y = \overline{(a_2, a_2)}y = \overline{(a_2, a_2)}\overline{(b_1, b_2)} = \overline{(a_2, a_2)(b_1, b_2)} = \overline{(a_2b_1, a_2b_2)} \end{cases}$$

Il suffit de prendre  $a = a_1b_2$ ,  $b = a_2b_1$ ,  $d = a_2b_2$  et on a :

$a, b, d \in A$  tels que :  $d \neq 0_A$ ,  $x = \overline{(a, d)}$  et  $y = \overline{(b, d)}$ .

- 10) Montrons par récurrence que pour tout entier naturel  $n \geq 2$ , si  $x_1, \dots, x_n$  sont des éléments quelconques de  $K$ , il existe des éléments  $a_1, \dots, a_n, d \in A$  tels que  $d \neq 0_A$  et  $\forall i = 1, \dots, n : x_i = \overline{(a_i, d)}$ .

– **Pour  $n = 2$  :**

Soient  $x_1, \dots, x_n$  des éléments quelconques de  $K$ .

D'après 9), il existe  $a_1, a_2, d \in A$  tels que,  $d \neq 0_A$ ,  $x_1 = \overline{(a_1, d)}$  et  $x_2 = \overline{(a_2, d)}$ .

Par suite il existe des éléments  $a_1, \dots, a_n, d \in A$  tels que :  $d \neq 0_A$  et

$\forall i = 1, \dots, n : x_i = \overline{(a_i, d)}$ .

– **Pour  $n - 1$  :**

Supposons que si  $x_1, \dots, x_{n-1}$  sont des éléments quelconques de  $K$ , il existe des éléments  $a_1, \dots, a_{n-1}, d \in A$  tels que :  $d \neq 0_A$  et  $\forall i = 1, \dots, n - 1 : x_i = \overline{(a_i, d)}$ .

– **Pour  $n$  :**

Montrons qu'alors si  $x_1, \dots, x_n$  sont des éléments quelconques de  $K$ , il existe des éléments  $a_1, \dots, a_n, d \in A$  tels que :  $d \neq 0_A$  et  $\forall i = 1, \dots, n : x_i = \overline{(a_i, d)}$ .

Soient  $x_1, \dots, x_n$  des éléments quelconques de  $K$ .

D'après l'hypothèse de récurrence, il existe des éléments  $a'_1, \dots, a'_{n-1}, d_1 \in A$  tels que,  $d_1 \neq 0_A$  et  $\forall i = 1, \dots, n - 1 : x_i = \overline{(a'_i, d_1)}$ .

$x_n \in K \Rightarrow \exists (a'_n, d_2) \in A \times A^* \text{ tq : } x_n = \overline{(a'_n, d_2)}$ .

$\forall i = 1, \dots, n :$

• **Si  $i \neq n$  :**

$$x_i = x_i\overline{(d_2, d_2)} = \overline{(a'_i, d_1)}\overline{(d_2, d_2)} = \overline{(a'_i, d_1)(d_2, d_2)} = \overline{(a'_id_2, d_1d_2)}.$$

Il suffit de prendre  $a_i = a'_id_2$ ,  $d = d_1d_2$  et on a :  $x_i = \overline{(a_i, d)}$ .

• **Si  $i = n$  :**

$$x_i = x_n = \overline{(d_1, d_1)}x_n = \overline{(d_1, d_1)}\overline{(a'_n, d_2)} = \overline{(d_1, d_1)(a'_n, d_2)} = \overline{(d_1a'_n, d_1d_2)}.$$

Il suffit de prendre  $a_i = a_n = d_1a'_n$ ,  $d = d_1d_2$  et on a :  $x_i = x_n = \overline{(a_i, d)}$ .

Ce qui montre que pour tout entier naturel  $n \geq 2$ , si  $x_1, \dots, x_n$  sont des éléments quelconques de  $K$ , il existe des éléments  $a_1, \dots, a_n, d \in A$  tels que,

$d \neq 0_A$  et  $\forall i = 1, \dots, n : x_i = \overline{(a_i, d)}$ .

- 11) • Soit  $g$  la relation de  $K \times K$  vers  $K$  définie par :

$\forall x, y, z \in K :$

$$(x, y)gz \Leftrightarrow [\exists a, b, d \in A \text{ tq : } d \neq 0_A, x = \overline{(a, d)}, y = \overline{(b, d)} \text{ et } z = \overline{(a + b, d)}]$$

Montrons que  $g$  est une loi de composition interne dans  $K$  qui sera noté additivement.

$$\begin{aligned}
& - \forall x, y, z, z' \in K \text{ tq : } (x, y)gz \text{ et } (x, y)gz'. \\
& \quad \exists a, b, d, a', b', d' \in A \text{ tq :} \\
& \quad d \neq 0_A, d' \neq 0_A, x = \overline{(a, d)} = \overline{(a', d')}, y = \overline{(b, d)} = \overline{(b', d')}, \\
& \quad z = \overline{(a + b, d)} \text{ et } z' = \overline{(a' + b', d')}. \\
& \quad x = \overline{(a, d)} = \overline{(a', d')} \Rightarrow (a, d)R_A(a', d') \Rightarrow ad' = da'. \\
& \quad y = \overline{(b, d)} = \overline{(b', d')} \Rightarrow (b, d)R_A(b', d') \Rightarrow bd' = db'. \\
& \quad \begin{cases} ad' = da' \\ bd' = db' \end{cases} \Rightarrow ad' + bd' = da' + db' \Rightarrow (a + b)d' = d(a' + b') \\
& \quad \Rightarrow (a + b, d)R_A(a' + b', d') \Rightarrow \overline{(a + b, d)} = \overline{(a' + b', d')} \\
& \quad \Rightarrow z = z'.
\end{aligned}$$

Donc  $g$  est une fonction de  $K \times K$  vers  $K$ .

$$- \forall (x, y) \in K \times K : \exists a, b, d \in A \text{ tq : } d \neq 0_A, x = \overline{(a, d)}, y = \overline{(b, d)}.$$

$$\text{Posons } z = \overline{(a + b, d)}. \begin{cases} x = \overline{(a, d)} \\ y = \overline{(b, d)} \\ z = \overline{(a + b, d)} \end{cases} \Rightarrow (x, y)gz \Rightarrow (x, y) \in D_g.$$

Donc  $D_g = K \times K$ . Par suite  $g$  est une application de  $K \times K$  vers  $K$ .

Ce qui montre que  $g$  est une loi de composition interne dans  $K$ .

La loi  $g$  est notée additivement.

- Montrons que :  $\forall a, b \in A \text{ et } \forall d \in A^* : \overline{(a, d)} + \overline{(b, d)} = \overline{(a + b, d)}$ .

Soient  $a, b, d$  des éléments quelconques de  $A$  tels que,  $d \neq 0_A$ .

Posons :  $x = \overline{(a, d)}, y = \overline{(b, d)}$  et  $z = \overline{(a + b, d)}$ .

$$\begin{aligned}
& \begin{cases} x = \overline{(a, d)} \\ y = \overline{(b, d)} \\ z = \overline{(a + b, d)} \end{cases} \Rightarrow (x, y)gz \Rightarrow g((x, y)) = z \Rightarrow x + y = z \\
& \Rightarrow \overline{(a, d)} + \overline{(b, d)} = \overline{(a + b, d)}.
\end{aligned}$$

- Soit  $\oplus$  une loi de composition interne quelconque dans  $K$  telle que :

$$\forall a, b \in A \text{ et } \forall d \in A^* : \overline{(a, d)} + \overline{(b, d)} = \overline{(a + b, d)}.$$

Soient  $x$  et  $y$  deux éléments quelconques de  $K$ .

$$\text{D'après 9) il existent des éléments } a, b \text{ et } d \text{ de } A \text{ tels que : } \begin{cases} x = \overline{(a, d)} \\ y = \overline{(b, d)} \end{cases}.$$

$$x \oplus y = \overline{(a, d)} \oplus \overline{(b, d)} = \overline{(a + b, d)} = \overline{(a, d)} + \overline{(b, d)} = x + y.$$

Ce qui montre qu'il existe une addition dans l'ensemble  $K = A \times A^* / R_A$

et une seule tel que :

$$\forall a, b \in A \text{ et } \forall d \in A^* : \overline{(a, d)} + \overline{(b, d)} = \overline{(a + b, d)}.$$

- 12) •  $\forall x, y \in K : \exists a, b, d \in A \text{ tq : } d \neq 0_A, x = \overline{(a, d)} \text{ et } y = \overline{(b, d)}.$

$$x + y = \overline{(a, d)} + \overline{(b, d)} = \overline{(a + b, d)} = \overline{(b + a, d)} = \overline{(b, d)} + \overline{(a, d)} = y + x.$$

Alors l'addition de  $K$  est commutative.

- $\forall x, y, z \in K : \exists a, b, c, d \in A \text{ tq : } d \neq 0_A, x = \overline{(a, d)}, y = \overline{(b, d)} \text{ et } z = \overline{(c, d)}.$

$$\begin{aligned}
(x + y) + z &= \overline{[(a, d) + (b, d)]} + \overline{(c, d)} = \overline{(a + b, d)} + \overline{(c, d)} = \overline{((a + b) + c, d)} \\
&= \overline{(a + (b + c), d)} = \overline{(a, d)} + \overline{(b + c, d)} = \overline{(a, d)} + \overline{[(b, d) + (c, d)]} \\
&= x + (y + z).
\end{aligned}$$

Alors l'addition de  $K$  est associative.

Ce qui montre que l'addition de  $K$  est commutative et associative.

$$\begin{aligned}
13) \quad \forall x, y, z \in K : \exists a, b, c, d \in A \text{ tq : } d \neq 0_A, x = \overline{(a, d)}, y = \overline{(b, d)} \text{ et } z = \overline{(c, e)}. \\
(x + y)z = \overline{[(a, d) + (b, d)](c, e)} = \overline{(a + b, d)(c, e)} = \overline{((a + b)c, de)} = \overline{(ac + bc, de)} \\
= \overline{(ac, de)} + \overline{(bc, de)} = \overline{(a, d)}\overline{(c, e)} + \overline{(b, d)}\overline{(c, e)} \\
= xz + yz.
\end{aligned}$$

Donc la multiplication de  $K$  est distributive par rapport à l'addition.

$$14) \quad \forall x \in K : \exists a, b \in A \text{ tq : } b \neq 0_A \text{ et } x = \overline{(a, b)}. \\
x + \overline{(0_A, u)} = \overline{(a, b)} + \overline{(0_A, u)} = \overline{(a, b)} + \overline{(0_A, b)} = \overline{(a + 0_A, b)} = \overline{(a, b)} = x.$$

Ce qui prouve que  $\overline{(0_A, u)}$  est le zéro de  $K$ .

15) Soit  $(a, b)$  un élément quelconque de  $A \times A^*$ .

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(a - a, b)} = \overline{(0_A, b)} = \overline{(0_A, u)}.$$

Alors  $\overline{(a, b)}$  admet un opposé et on a :  $-\overline{(a, b)} = \overline{(-a, b)}$ .

16) • ★ L'addition est commutative et associative.

★  $K$  admet un zéro, qui est  $\overline{(0_A, u)}$ .

$$\begin{aligned}
\star \quad \forall x \in K : \exists a, b \in A \text{ tq : } b \neq 0_A \text{ et } x = \overline{(a, b)}. \\
x = \overline{(a, b)} \text{ admet un opposé, qui est } \overline{(-a, b)}.
\end{aligned}$$

Donc  $(K, +)$  est un groupe abélien et on a :  $0_K = \overline{(0_A, u)}$ .

• ★ La multiplication est commutative et associative dans  $K$ .

★ La multiplication est distributive par rapport à l'addition dans  $K$ .

★  $K$  admet un élément neutre pour la multiplication, qui est  $\overline{(u, u)}$ .

★  $u \neq 0_A \Rightarrow \overline{(u, u)} \neq \overline{(0_A, u)} = 0_K$ .

Alors  $(K, +, \cdot)$  est un anneau abélien unitaire non nul et on a :  $1_K = \overline{(u, u)}$ .

$$\begin{aligned}
\bullet \quad \forall x \in K^* : \exists a, b \in A \text{ tq : } b \neq 0_A \text{ et } x = \overline{(a, b)}. \\
\overline{(a, b)} = x \neq 0_K = \overline{(0_A, u)} \Rightarrow a \neq 0_A \text{ (d'après 3)).}
\end{aligned}$$

D'après 8), on a donc  $x = \overline{(a, b)}$  est inversible.

Alors :  $U(K) = K^*$ .

Ce qui montre que  $K$  est un corps commutatif.

17) •  $\forall a, b \in A :$

$$\varphi(a + b) = \overline{((a + b)u, u)} = \overline{(au + bu, u)} = \overline{(au, u)} + \overline{(bu, u)} = \varphi(a) + \varphi(b).$$

$$\begin{aligned}
\varphi(ab) &= \overline{((ab)u, u)} = \overline{(abu, u)} = \overline{(abu, u)}1_K = \overline{(aub, u)(u, u)} = \overline{(aubu, uu)} \\
&= \overline{((au)(bu), uu)} = \overline{(au, u)}\overline{(bu, u)} \\
&= \varphi(a)\varphi(b).
\end{aligned}$$

Donc  $\varphi$  est un homomorphisme de  $(A, +, \cdot)$  vers  $(K, +, \cdot)$ .

$$\bullet \quad \forall a \in \ker \varphi : \overline{(au, u)} = \varphi(a) = 0_K = \overline{(0_A, u)} \Rightarrow au = 0_A \Rightarrow a = 0_A \text{ (car } u \neq 0_A).$$

Par suite on a :  $\ker \varphi = \{0_A\}$ .

Ce qui montre que  $\varphi$  est un homomorphisme injectif de  $(A, +, \cdot)$  vers  $(K, +, \cdot)$ .

Par la suite on confond chaque élément  $a$  de  $A$  avec  $\varphi(a)$ .

18)  $\varphi(A) = A$  (car d'après 17), on a confondu chaque élément  $a$  de  $A$  avec  $\varphi(a)$ ).

Puisque  $A$  est un anneau et puisque  $\varphi$  est un homomorphisme de  $(A, +, \cdot)$

vers  $(K, +, \cdot)$  alors  $A = \varphi(A)$  est un sous-anneau de  $K$ .

19)  $\forall (a, b) \in A \times A^* :$

$$\begin{aligned}
\overline{(a, b)} &= \overline{(a, b)}1_K = \overline{(a, b)(uu, uu)} = \overline{(auu, buu)} = \overline{(auu, ubu)} = \overline{((au)u, u(bu))} \\
&= \overline{(au, u)(u, bu)} = \overline{(au, u)}\overline{(bu, u)}^{-1} = \varphi(a)[\varphi(b)]^{-1} = ab^{-1} \\
&= \frac{a}{b}.
\end{aligned}$$

$$20) \quad K = \left\{ \overline{(a, b)} \text{ tq : } a, b \in A \text{ et } b \neq 0_A \right\} = \left\{ \frac{a}{b} \text{ tq : } a, b \in A \text{ et } b \neq 0_A \right\}$$

Alors  $K$  est le corps des fractions de  $A$  dans  $K$ .

Ce qui montre que  $K$  est un corps des fractions de  $A$ .

**Définition 4-4-6 :**

Soit  $A$  un anneau, et soient  $E$  et  $F$  deux sur-anneaux de

- ★ Si  $f$  est un isomorphe d'anneaux de  $E$  vers  $F$ , et si on a :  $\forall a \in A : f(a) = a$ , on dit que  $f$  est un  $A$ -isomorphe de  $E$  vers  $F$ .
- ★ S'il existe un  $A$ -isomorphisme de  $E$  vers  $F$ , on dit que  $E$  est  $A$ -isomorphe à  $F$  ou  $E$  et  $F$  sont  $A$ -isomorphes.

**Théorème et définition 4-4-7 :**

Tout anneau commutatif intègre non nul  $A$  admet un corps des fractions et un seul à  $A$ -isomorphe près.

**Démonstration :**

Soit  $A$  un anneau commutatif intègre non nul.

**– Existence :**

D'après la propriété 20) théorème 4-4-5,  $A$  admet au moins un corps des fractions.

**– Unicité :**

Soient  $(K, \oplus, \otimes)$  et  $(M, \mp, \odot)$  deux corps de fractions de  $A$ .

$$\begin{cases} \forall x \in K^* : \text{l'inverse de } x \text{ dans } K \text{ est noté } \tilde{x} \\ \forall x \in M^* : \text{l'inverse de } x \text{ dans } M \text{ est noté } \bar{x} \end{cases}$$

Puisque  $(K, \oplus, \otimes)$  et  $(M, \mp, \odot)$  des corps de fractions de  $A$  alors :

$$K = \{a \otimes \tilde{b} \text{ tq : } a, b \in A \text{ et } b \neq 0_A\} \quad \text{et} \quad M = \{a \odot \bar{b} \text{ tq : } a, b \in A \text{ et } b \neq 0_A\}.$$

Soit  $h$  la relation de  $K$  vers  $M$  définies par :

$$\forall x \in K \text{ et } \forall y \in M : xhy \Leftrightarrow [\exists a, b \in A \text{ tq : } b \neq 0_A \text{ } x = a \otimes \tilde{b} \text{ et } y = a \odot \bar{b}].$$

- Montrons que  $h$  est une fonction de  $K$  vers  $M$ .

$$\forall x \in K \quad \text{et} \quad \forall y, y' \in M \text{ tq : } [xhy \quad \text{et} \quad xhy'].$$

$$\begin{cases} xhy \Rightarrow [\exists a, b \in A \text{ tq : } b \neq 0_A \text{ } x = a \otimes \tilde{b} \text{ et } y = a \odot \bar{b}] \\ xhy' \Leftrightarrow [\exists a', b' \in A \text{ tq : } b' \neq 0_A \text{ } x = a' \otimes \tilde{b}' \text{ et } y' = a' \odot \bar{b}'] \end{cases}$$

$$\begin{aligned} \text{Alors : } a \otimes \tilde{b} = x = a' \otimes \tilde{b}' &\Rightarrow (a \otimes \tilde{b}) \otimes b \otimes b' = a' \otimes \tilde{b}' \otimes b \otimes b' \\ &\Rightarrow (a \otimes \tilde{b}) \otimes b \otimes b' = a' \otimes \tilde{b}' \otimes b' \otimes b \\ &\Rightarrow a \otimes (\tilde{b} \otimes b) \otimes b' = a' \otimes (\tilde{b}' \otimes b') \otimes b \\ &\Rightarrow a \otimes 1_K \otimes b' = a' \otimes 1_K \otimes b \\ &\Rightarrow a \otimes b' = a' \otimes b \Rightarrow ab' = a'b \Rightarrow a \odot b' = a' \odot b \\ &\Rightarrow (a \odot b') \odot (\bar{b} \odot \bar{b}') = (a' \odot b) \odot (\bar{b} \odot \bar{b}') \\ &\Rightarrow (a \odot b') \odot (\bar{b}' \odot \bar{b}) = (a' \odot b) \odot (\bar{b} \odot \bar{b}') \\ &\Rightarrow a \odot (b' \odot \bar{b}') \odot \bar{b} = a' \odot (b \odot \bar{b}) \odot \bar{b}' \\ &\Rightarrow a \odot 1_M \odot \bar{b} = a' \odot 1_M \odot \bar{b}' \Rightarrow a \odot \bar{b} = a' \odot \bar{b}' \\ &\Rightarrow y = y'. \end{aligned}$$

Donc  $h$  est une fonction de  $K$  vers  $M$ .

- Montrons que  $h$  est une application de  $K$  vers  $M$ .

$$\forall x \in K : \exists a, b \in A \text{ tq : } b \neq 0_A \text{ et } x = a \otimes \tilde{b}.$$

$$\text{Posons } y = a \odot \bar{b}.$$

$$[a, b \in A, b \neq 0_A, x = a \otimes \tilde{b} \text{ et } y = a \odot \bar{b}] \Rightarrow xhy \Rightarrow x \in D_h.$$

Alors  $D_h = K$ . Donc  $h$  est une application de  $K$  vers  $M$ .

- Montrons que :  $\forall a, b \in A \text{ tq : } b \neq 0_A$ , on a :  $h(a \otimes \tilde{b}) = a \odot \bar{b}$ .

$$\forall a, b \in A \text{ tq : } b \neq 0_A :$$

$$\text{Posons : } x = a \otimes \tilde{b} \text{ et } y = a \odot \bar{b}. \text{ Alors : } x \in K, y \in M \text{ et } xhy.$$

$$\text{Donc : } h(a \otimes \tilde{b}) = h(x) = y = a \odot \bar{b}.$$

- Montrons que :  $\forall a \in A : h(a) = a$ .

Soit  $u$  un élément non nul de  $A$  ( $u$  existe car  $A$  est non nul).

$$\begin{aligned} \forall a \in A : h(a) &= h(a \otimes 1_K) = h(a \otimes (u \otimes \tilde{u})) = h((a \otimes u) \otimes \tilde{u}) = h((au) \otimes \tilde{u}) \\ &= (au) \odot \bar{u} = (a \odot u) \odot \bar{u} = a \odot (u \odot \bar{u}) = a \odot 1_M \\ &= a \end{aligned}$$

$$\begin{cases} a = a1_A = a \otimes 1_K = a \otimes (u \otimes \tilde{u}) = (a \otimes u) \otimes \tilde{u} = (au) \otimes \tilde{u} \\ a = a1_A = a \odot 1_M = a \odot (u \odot \bar{u}) = (a \odot u) \odot \bar{u} = (au) \odot \bar{u} \end{cases}.$$

$$\text{Alors : } aha \Rightarrow h(a) = a.$$

- Montrons que :  $\forall x, y \in K : \exists a, b, d \in A \text{ tq : } d \neq 0_A, x = a \otimes \tilde{d} \text{ et } y = b \otimes \tilde{d}$ .

$$\forall x, y \in K : \exists a_1, a_2, b_1, b_2 \in A \text{ tq : } a_2 \neq 0_A, b_2 \neq 0_A, x = a_1 \otimes \tilde{a_2} \text{ et } y = b_1 \otimes \tilde{b_2}.$$

$$\text{Alors : } x = a_1 \otimes \tilde{a_2} = a_1 \otimes 1_K \otimes \tilde{a_2} = a_1 \otimes (b_2 \otimes \tilde{b_2}) \otimes \tilde{a_2}$$

$$= (a_1 \otimes b_2) \otimes (\tilde{b_2} \otimes \tilde{a_2}) = (a_1 b_2) \otimes (\widetilde{a_2 \otimes b_2})$$

$$= (a_1 b_2) \otimes (\widetilde{a_2 b_2})$$

$$y = b_1 \otimes \tilde{b_2} = b_1 \otimes 1_K \otimes \tilde{b_2} = b_1 \otimes (a_2 \otimes \tilde{a_2}) \otimes \tilde{b_2}$$

$$= (b_1 \otimes a_2) \otimes (\tilde{a_2} \otimes \tilde{b_2}) = (b_1 a_2) \otimes (\widetilde{b_2 \otimes a_2}) = (b_1 a_2) \otimes (\widetilde{b_2 a_2})$$

$$= (b_1 a_2) \otimes (\widetilde{a_2 b_2})$$

Il suffit de prendre :  $a = a_1 b_2, b = b_1 a_2, d = a_2 b_2$  et on a :

$$a, b, d \in A, \quad d \neq 0_A, \quad x = a \otimes \tilde{d} \quad \text{et} \quad y = b \otimes \tilde{d}.$$

- Montrons que  $h$  est un homomorphisme de  $(K, \oplus)$  vers  $(M, \mp)$ .

$$\forall x, y \in K : \exists a, b, d \in A \text{ tq : } d \neq 0_A, x = a \otimes \tilde{d} \text{ et } y = b \otimes \tilde{d}.$$

$$\begin{aligned} h(x \oplus y) &= h((a \otimes \tilde{d}) \oplus (b \otimes \tilde{d})) = h((a \oplus b) \otimes \tilde{d}) = h((a + b) \otimes \tilde{d}) \\ &= (a + b) \odot \bar{d} = (a \mp b) \odot \bar{d} = (a \odot \bar{d}) \mp (b \odot \bar{d}) = h(a \otimes \tilde{d}) \mp h(b \otimes \tilde{d}) \\ &= h(x) \mp h(y). \end{aligned}$$

Donc  $h$  est un homomorphisme de  $(K, \oplus)$  vers  $(M, \mp)$ .

- Montrons que  $h$  est un homomorphisme de  $(K, \otimes)$  vers  $(M, \odot)$ .

$$\forall x, y \in K : \exists a, b, c, d \in A \text{ tq : } b \neq 0_A, d \neq 0_A, x = a \otimes \tilde{b} \text{ et } y = c \otimes \tilde{d}.$$

$$\begin{aligned} h(x \otimes y) &= h((a \otimes \tilde{b}) \otimes (c \otimes \tilde{d})) = h(a \otimes \tilde{b} \otimes c \otimes \tilde{d}) = h(a \otimes c \otimes \tilde{d} \otimes \tilde{b}) \\ &= h((a \otimes c) \otimes (\tilde{d} \otimes \tilde{b})) = h((a \otimes c) \otimes \widetilde{b \otimes d}) = h((ac) \otimes \widetilde{bd}) \\ &= (ac) \odot \overline{bd} = (a \odot c) \odot \overline{b \odot d} = (a \odot c) \odot (\bar{d} \odot \bar{b}) = a \odot c \odot \bar{d} \odot \bar{b} \\ &= a \odot \bar{b} \odot c \odot \bar{d} = (a \odot \bar{b}) \odot (c \odot \bar{d}) = h(a \otimes \tilde{b}) \odot h(c \otimes \tilde{d}) \\ &= h(x) \odot h(y). \end{aligned}$$

Donc  $h$  est un homomorphisme de  $(K, \otimes)$  vers  $(M, \odot)$ .

- Alors  $h$  est un homomorphisme d'anneaux de  $(K, \oplus, \otimes)$  vers  $(M, \mp, \odot)$ .

- Puisque  $h(A) = A$  (car on a :  $\forall a \in A : h(a) = a$ ) et puisque  $A$  est non nul alors  $h$  est non nul.  
Puisque  $K$  est un corps et puisque  $h$  est non nul, alors  $h$  est injectif.
- $\forall y \in M : \exists a, b \in A$  tq :  $b \neq 0_A$  et  $y = a \odot \bar{b}$ .  
Alors :  $y = a \odot \bar{b} = h(a \otimes \tilde{b})$ .  
Donc  $h$  est surjectif.
- Par suite  $h$  est un  $A$ -isomorphe de  $K$  vers  $M$ .  
Ce qui montre que  $K$  et  $M$  sont  $A$ -isomorphes.  
D'où l'unicité du corps de fractions de  $A$  à  $A$ -isomorphe près.

#### Exemple 4-4-8 :

- ★  $\mathbb{Q}$  est le corps des fractions de  $\mathbb{Z}$ .
- ★ Pour tout entier naturel non nul  $n$ ,  $\mathbb{Q}$  est le corps des fractions de  $n\mathbb{Z}$ .

#### 4-5-Idéaux :

##### Définition 4-5-1 :

Soient  $A$  un anneau et  $I$  une partie de  $A$ . On dit que  $I$  est un idéal de  $A$ , si  $I$  est un sous groupe de  $(A, +)$  et si on a :  $\forall a \in A$  et  $\forall x \in I : ax, xa \in I$ .

##### Exemples et propriétés 4-5-2 :

Soit  $A$  un anneau.

- 1) Les idéaux de  $\mathbb{Z}$  sont les parties de  $\mathbb{Z}$  de la forme  $n\mathbb{Z}$  telle que  $n \in \mathbb{N}$ .
- 2)  $\{0_A\}$  et  $A$  sont des idéaux de  $A$  appelés les idéaux triviaux de  $A$ .  
 $\{0_A\}$  est appelé l'idéal nul de  $A$ .
- 3) Si  $A$  est unitaire et si  $I$  est un idéal de  $A$  alors  $I = A$  si et seulement si  $1 \in I$ .
- 4) Si  $A$  est un corps, les seuls idéaux de  $A$  sont  $\{0_A\}$  et  $A$ .
- 5) Les idéaux de  $A$  sont tous des sous-anneaux de  $A$ .
- 6) Si  $A = \mathbb{Q}$ .
  - i) Les seuls idéaux de  $\mathbb{Q}$  sont  $\{0\}$  et  $\mathbb{Q}$ .
  - ii)  $\mathbb{Z}$  est un sous-anneaux de  $\mathbb{Q}$  qui n'est pas un idéal de  $\mathbb{Q}$ .
- 7) Si  $I$  et  $J$  sont des idéaux de  $A$  alors  $I \cap J$  et  $I + J$  sont des idéaux de  $A$ .
- 8) Si  $E$  est un ensemble non vide d'idéaux de  $A$  alors  $\bigcap_{I \in E} I$  est un idéal de  $A$ .
- 9) Si  $K$  est un ensemble non vide et si  $(I_k)_{k \in K}$  est une famille d'idéaux de  $A$  indexé par  $K$ , alors  $\bigcap_{k \in K} I_k$  est un idéal de  $A$ .
- 10) Soit  $a$  un élément quelconque de  $A$ .
  - i) Si  $A$  est abélien alors  $aA = Aa = \{ax \text{ tq } x \in A\}$  est un idéal de  $A$ .
  - ii) Si  $A$  est abélien unitaire alors l'idéal  $aA = Aa$  contient  $a$  et c'est le petit idéal de  $A$  contenant  $a$ .  
On dit que  $aA = Aa$  est l'idéal de  $A$  engendré par  $a$ .  
 $aA = Aa$  est noté aussi  $(a)$  (c'est à dire  $(a) = aA = Aa$ ).
- 11) Si  $A$  est unitaire et si  $I$  est un idéal de  $I$  de  $A$  alors :  
 $\forall a \in A : a \in I \Leftrightarrow aA \subset I \Leftrightarrow Aa \subset I$ .
- 12) Si  $A$  est abélien unitaire non nul alors  $A$  est un corps si et seulement si les seuls idéaux de  $A$  sont  $\{0_A\}$  et  $A$ .



- 13) Si  $A$  est unitaire et si  $I$  est une partie quelconque de  $A$  alors  $I$  est un idéal de  $A$  si et seulement si on a les trois propriétés suivantes :
- i)  $I \neq \emptyset$ .
  - ii)  $\forall x, y \in I : x + y \in I$ .
  - iii)  $\forall a \in A$  et  $\forall x \in I : ax \in I$ .
- 14) Soit  $B$  un autre anneau et  $f$  est un homomorphisme d'anneaux de  $A$  vers  $B$ .
- i) Si  $J$  est un idéal de  $B$  alors  $f^{-1}(J)$  est un idéal de  $A$ .
  - ii)  $\ker f$  est un idéal de  $A$  (car  $\ker f = f^{-1}(\{0_B\})$ )
  - iii) Si  $f$  est surjectif et si  $I$  est un idéal de  $A$  alors  $f(I)$  est un idéal de  $B$ .
  - iv) Si  $A$  est un corps et si  $f$  est non nul alors  $f$  est injectif.

### Démonstration :

- 1) Soit  $I$  une partie quelconque de  $\mathbb{Z}$ .

$\Rightarrow$  ) **Si  $I$  est un idéal de  $\mathbb{Z}$  :**

Alors  $I$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

Donc il existe un entier naturel  $n$  tel que  $I = n\mathbb{Z}$ .

$\Leftarrow$  ) **S'il existe un entier naturel  $n$  tel que  $I = n\mathbb{Z}$  :**

•  $I = n\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

•  $\forall a \in \mathbb{Z}$  et  $\forall x \in I = n\mathbb{Z} : \exists k \in \mathbb{Z} \text{ tq } x = nk$ .

Alors :  $ax = xa = a(nk) = (nk)a = n(ka) \in I = n\mathbb{Z}$ .

Donc  $I = n\mathbb{Z}$  est un idéal de  $\mathbb{Z}$ .

Ce qui montre que les idéaux de  $\mathbb{Z}$  sont les parties de  $\mathbb{Z}$  de la forme  $n\mathbb{Z}$  telle que  $n \in \mathbb{N}$ .

- 2) •  $\star \{0_A\}$  est un sous-groupe de  $(A, +)$ .

•  $\star A$  est un sous-groupe de  $(A, +)$ .

$\star \forall a \in A$  et  $\forall x \in \{0_A\} : x = 0_A$ .

$$\begin{cases} ax = a0_A = 0_A \in \{0_A\} \\ xa = 0_Aa = 0_A \in \{0_A\} \end{cases} \Rightarrow ax = xa \in \{0_A\}.$$

Donc  $\{0_A\}$  est un idéal de  $A$ .

•  $\star A$  est un sous-groupe de  $(A, +)$ .

$\star \forall a \in A$  et  $\forall x \in A : ax, xa \in A$ .

Donc  $A$  est un idéal de  $A$ .

Ce qui montre que  $\{0_A\}$  et  $A$  sont des idéaux de  $A$ .

$\{0_A\}$  est appelé l'idéal nul de  $A$ .

- 3)  $\Rightarrow$  ) **Si  $I = A$  :**

Alors  $1 \in A = I$ .

$\Leftarrow$  ) **Si  $1 \in I$  :**

$\forall x \in A : x = x1 \in I$  (car  $1 \in I$ ). Donc  $I = A$ .

- 4) Supposons que  $A$  est un corps et que  $I$  est un idéal non nul de  $A$ .

Alors  $I$  admet au moins un élément non nul  $a$ .

Puisque  $a \in I$  alors  $1 = aa^{-1} \in I$  ( $a^{-1}$  existe car  $a \neq 0$  et  $A$  est un corps).

Donc  $I = A$ .

Ce qui montre que les seuls idéaux de  $A$  sont  $\{0_A\}$  et  $A$ .

5) Soit  $I$  un idéal quelconque de  $A$ .

- $I$  est un sous-groupe de  $(A, +)$ .
- $\forall a, b \in I : [a \in A \quad \text{et} \quad b \in I] \Rightarrow ab \in I$ .

Alors  $I$  est sous-anneau de  $A$ .

Ce qui montre que les idéaux de  $A$  sont tous des sous-anneaux de  $A$ .

6) Si  $A = \mathbb{Q}$ .

- i) Les seuls idéaux de  $\mathbb{Q}$  sont  $\{0\}$  et  $\mathbb{Q}$  (car  $\mathbb{Q}$  est un corps).
- ii)  $\mathbb{Z}$  est un sous-anneaux de  $\mathbb{Q}$  qui n'est pas un idéal de  $\mathbb{Q}$  (d'après i)).

7) Soient  $I$  et  $J$  deux idéaux de  $A$ .

- $I \cap J$  et  $I + J$  sont des sous-groupes de  $(A, +)$ .
- $\forall a \in A \quad \text{et} \quad \forall x \in I \cap J :$   

$$x \in I \cap J \Rightarrow [x \in I \quad \text{et} \quad x \in J] \Rightarrow [ax, xa \in I \quad \text{et} \quad ax, xa \in J] \Rightarrow ax, xa \in I \cap J.$$
- $\forall a \in A \quad \text{et} \quad \forall x \in I + J : \exists u \in I \quad \text{et} \quad \exists v \in J \text{ tq : } x = u + v.$   

$$\begin{cases} ax = a(u + v) = au + av \in I + J \\ xa = (u + v)a = ua + va \in I + J \end{cases} \Rightarrow ax, xa \in I + J.$$

Donc  $I \cap J$  et  $I + J$  sont des idéaux de  $A$ .

8) Soit  $E$  un ensemble non vide d'idéaux de  $A$ .

- $\bigcap_{I \in E} I$  est un sous-groupe de  $(A, +)$ .
- $\forall a \in A \quad \text{et} \quad \forall x \in \bigcap_{I \in E} I :$   

$$x \in \bigcap_{I \in E} I \Rightarrow [\forall I \in E : x \in I] \Rightarrow [\forall I \in E : ax, xa \in I] \Rightarrow ax, xa \in \bigcap_{I \in E} I.$$

Donc  $\bigcap_{I \in E} I$  est un idéal de  $A$ .

9) Soient  $K$  un ensemble non vide et  $(I_k)_{k \in K}$  une famille d'idéaux de  $A$  indexé par  $K$ .

- $\bigcap_{k \in K} I_k$  est un sous-groupe de  $(A, +)$ .
- $\forall a \in A \quad \text{et} \quad \forall x \in \bigcap_{k \in K} I_k :$   

$$x \in \bigcap_{k \in K} I_k \Rightarrow [\forall k \in K : x \in I_k] \Rightarrow [\forall k \in K : ax, xa \in I_k] \Rightarrow ax, xa \in \bigcap_{k \in K} I_k.$$

Donc  $\bigcap_{k \in K} I_k$  est un idéal de  $A$ .

10) i) Supposons que  $A$  est abélien.

- $\star \quad 0_A = a0_A \in aA \Rightarrow aA = Aa \neq \emptyset.$
- $\star \quad \forall x, y \in aA : \exists u, v \in A \text{ tq : } x = au \quad \text{et} \quad y = av.$   

$$x - y = au - av = a(u - v) \in aA.$$

Donc  $aA = Aa$  est un sous-groupe de  $(A, +)$ .

- $\forall b \in A \quad \text{et} \quad \forall x \in aA : \exists u \in A \text{ tq : } x = au.$   

$$bx = b(au) = (au)b = a(bu) \in aA.$$

Ce qui prouve que  $aA = Aa$  est un idéal de  $A$ .

ii) Supposons que  $A$  est abélien unitaire.

- $a = a1_A \in aA.$
- Soit  $I$  un idéal quelconque de  $A$  contenant  $a$ .

$$\forall x \in aA : \exists u \in A \text{ tq : } x = au. \quad \begin{cases} u \in A \\ a \in I \end{cases} \Rightarrow x = au \in I. \text{ Alors } aA \subset I.$$

Donc  $aA = Aa$  est le petit idéal de  $A$  contenant  $a$ .

11) Supposons que  $A$  est unitaire et que  $I$  est un idéal de  $A$ .

Soit  $a$  un élément quelconque de  $A$ .

– **Si  $a \in I$  :**

★  $\forall x \in aA : \exists u \in A \text{ tq } : x = au$ . Alors :  $x = au \in I$  (car  $a \in I$  et  $u \in A$ ).

★  $\forall x \in Aa : \exists u \in A \text{ tq } : x = ua$ . Alors :  $x = ua \in I$  (car  $a \in I$  et  $u \in A$ ).

Alors :  $aA \subset I$  et  $Aa \subset I$ .

– **Si  $aA \subset I$  :**

Alors :  $a = a1_A \in aA \subset I \Rightarrow a \in I$ .

– **Si  $Aa \subset I$  :**

Alors :  $a = 1_A a \in Aa \subset I \Rightarrow a \in I$ .

Ce qui montre que :  $a \in I \Leftrightarrow aA \subset I \Leftrightarrow Aa \subset I$ .

12) Supposons que  $A$  est abélien unitaire non nul.

$\Rightarrow$  ) **Si  $A$  est un corps :**

D'après 4), les seuls idéaux de  $A$  sont  $\{0_A\}$  et  $A$ .

$\Leftarrow$  ) **Si les seuls idéaux de  $A$  sont  $\{0_A\}$  et  $A$  :**

Soit  $a$  un élément non nul quelconque de  $A$ .

Puisque  $aA$  est un idéal non nul de  $A$  alors  $aA = A$ .

Alors :  $1 \in A = aA \Rightarrow \exists a' \in A \text{ tq } : aa' = 1 \Rightarrow a$  est inversible dans  $A$ .

Ce qui montre que  $A$  est un corps.

13) Supposons que  $A$  est unitaire et soit  $I$  est une partie quelconque de  $A$ .

$\Rightarrow$  ) **Si  $I$  est un idéal de  $A$  :**

Alors les trois propriétés i), ii) et iii) sont vérifiées.

$\Leftarrow$  ) **Si les trois propriétés i), ii) et iii) sont vérifiées :**

$\forall x \in I : -x = -(1_A x) = (-1_A)x \in I$  (d'après iii)).

Puisque les deux propriétés i) et ii) sont vérifiées et puisque l'opposé de tout élément de  $I$  est un élément de  $I$  alors  $I$  est un sous-groupe de  $(A, +)$ .

Puisque  $I$  est un sous-groupe de  $(A, +)$  et puisque iii) est vérifiée alors  $I$  est un idéal de  $A$ .

14) Soit  $B$  un autre anneau et  $f$  est un homomorphisme d'anneaux de  $A$  vers  $B$ .

i) Soit  $J$  un idéal de  $B$ .

•  $f^{-1}(J)$  est un sous-groupe de  $(A, +)$  (car  $J$  est un sous-groupe de  $(B, +)$ ).

•  $\forall a \in A \text{ et } \forall x \in f^{-1}(J) : f(x) \in J$ .

$$\text{Alors : } \begin{cases} f(ax) = f(a)f(x) \in J \Rightarrow ax \in f^{-1}(J) \\ f(xa) = f(x)f(a) \in J \Rightarrow xa \in f^{-1}(J) \end{cases} \Rightarrow ax, xa \in f^{-1}(J).$$

Donc  $f^{-1}(J)$  est un idéal de  $A$ .

ii) Puisque  $\{0_B\}$  est un idéal de  $B$ , alors (d'après i)),  $\ker f = f^{-1}(\{0_B\})$  est un idéal de  $A$ .

iii) Supposons que  $f$  est surjectif et que  $I$  est un idéal de  $A$ .

•  $f(I)$  est un sous-groupe de  $(B, +)$  (car  $I$  est un sous-groupe de  $(A, +)$ ).

•  $\forall b \in B \text{ et } \forall y \in f(I) : \exists a \in A, \text{ et } \exists x \in I \text{ tq } : b = f(a) \text{ et } y = f(x)$ .

$$[a \in A \text{ et } x \in I] \Rightarrow ax, xa \in I.$$

$$\text{Alors : } \begin{cases} by = f(a)f(x) = f(ax) \in f(I) \\ yb = f(x)f(a) = f(xa) \in f(I) \end{cases} \Rightarrow by, yb \in f(I).$$

Donc  $f(I)$  est un idéal de  $B$ .

iv) Supposons que  $A$  est un corps et que  $f$  est non nul.

Puisque  $f$  est non nul alors  $\ker f \neq A$ . Donc  $\ker f$  est nul (car  $A$  est un corps).

Ce qui montre que  $f$  est injectif.

**Définition 4-5-3 :**

Soient  $A$  un anneau et  $I$  un idéal de  $A$ . On dit que :

- ★  $I$  est un idéal premier de  $A$ , si on a :  $\forall x, y \in A : xy \in I \Rightarrow [x \in I \text{ ou } y \in I]$ .
- ★  $I$  est un idéal maximal de  $A$ , si  $I$  est un élément maximal (pour l'inclusion) de l'ensemble des idéaux de  $A$  distincts de  $A$ . C'est à dire si :  
 $I \neq A$  et si pour tout idéal  $J$  de  $A$  on a :  $I \subset J \Rightarrow [J = I \text{ ou } J = A]$ .

**Exemples et propriétés 4-5-4 :**

Soit  $A$  un anneau.

- 1)  $A$  est un idéal premier de  $A$  lui même, mais  $A$  n'est pas un idéal maximal de  $A$ .
- 2)  $\{0_A\}$  est un idéal premier de  $A$  si et seulement si  $A$  est intègre.
- 3) Si  $A$  est un corps alors  $\{0_A\}$  est un idéal maximal de  $A$ .
- 4) Si  $A$  est commutatif unitaire alors  $\{0_A\}$  est un idéal maximal de  $A$  si et seulement si  $A$  est un corps.
- 5) Les idéaux premiers de  $\mathbb{Z}$  sont  $\{0\}$ ,  $\mathbb{Z}$  et les idéaux de  $p\mathbb{Z}$  tels  $p$  soit un nombre premier.
- 6) Les idéaux maximaux de  $\mathbb{Z}$  sont les idéaux  $p\mathbb{Z}$  tels  $p$  soit un nombre premier.
- 7) Soit  $B$  un autre anneau et  $f$  est un homomorphisme d'anneaux de  $A$  vers  $B$ .  
 Si  $J$  est un idéal premier de  $B$  alors  $f^{-1}(J)$  est un idéal premier de  $A$ .

**Démonstration :**

- 1) •  $A$  est un idéal premier de  $A$  lui même, car on a :  
 $\forall x, y \in A : xy \in A \Rightarrow x \in A \text{ ou } y \in A$ .  
 •  $A$  n'est pas un idéal maximal de  $A$ , car  $A$  n'appartient pas à l'ensemble des idéaux de  $A$  distincts de  $A$ .
- 2)  $\Rightarrow$  ) **Si  $\{0_A\}$  est un idéal premier de  $A$  :**  
 $\forall x, y \in A \text{ tq : } xy = 0_A$ .  
 $xy = 0_A \Rightarrow xy \in \{0_A\}$   
 $\Rightarrow [x \in \{0_A\} \text{ ou } y \in \{0_A\}]$  (car  $\{0_A\}$  est un idéal premier de  $A$ )  
 $\Rightarrow [x = 0_A \text{ ou } y = 0_A]$ .  
 Donc  $A$  est intègre.  
 $\Leftarrow$  ) **Si  $A$  est intègre :**  
 $\forall x, y \in A \text{ tq : } xy \in \{0_A\}$ .  
 $xy \in \{0_A\} \Rightarrow xy = 0_A$   
 $\Rightarrow [x = 0_A \text{ ou } y = 0_A]$  (car  $A$  est un anneau intègre)  
 $\Rightarrow [x \in \{0_A\} \text{ ou } y \in \{0_A\}]$ .  
 Donc  $\{0_A\}$  est un idéal premier de  $A$ .
- 3) Supposons que  $A$  est un corps.  
 Puisque  $A$  est un corps alors  $\{0_A\} \neq A$ . Soit  $J$  un idéal de  $A$  contenant  $\{0_A\}$ .  
 Par suite  $J = \{0_A\}$  ou  $J = A$  (car  $A$  est un corps).  
 Donc  $\{0_A\}$  est un idéal maximal de  $A$ .
- 4) Supposons que  $A$  est commutatif unitaire.  
 $\Leftarrow$  ) **Si  $A$  est un corps :**  
 Alors (d'après la propriété précédente)  $\{0_A\}$  est un idéal maximal de  $A$ .

⇒ ) **Si  $\{0_A\}$  est un idéal maximal de  $A$  :**

Soit  $I$  un idéal quelconque de  $A$ .

Puisque  $\{0_A\} \subset I$  et puisque  $\{0_A\}$  est un idéal maximal de  $A$  alors  $I = \{0_A\}$  ou  $I = A$ . Donc  $\{0_A\}$  et  $A$  sont les seuls idéaux de  $A$ .

Ce qui montre (d'après la propriété 4-5-2-12) que  $A$  est un corps.

5) Supposons que  $A = \mathbb{Z}$

- $\{0\} = 0\mathbb{Z}$  est un idéal premier de  $\mathbb{Z}$  (car  $\mathbb{Z}$  est un anneau intègre).

- $\mathbb{Z} = 1\mathbb{Z}$  est un idéal premier de  $\mathbb{Z}$

- Soit  $p$  un entier naturel quelconque tel que  $p \neq 0$  et  $p \neq 1$

Montrons que  $p\mathbb{Z}$  est un idéal premier de  $\mathbb{Z}$  si et seulement si  $p$  est un nombre premier.

⇒ ) **Si  $p\mathbb{Z}$  est un idéal premier de  $\mathbb{Z}$  :**

Soit  $q$  un diviseur quelconque de  $p$ .

Alors il existe un entier naturel  $q'$  tel que  $qq' = p$ .

$$qq' = p \Rightarrow qq' \in p\mathbb{Z}$$

$$\Rightarrow [q \in p\mathbb{Z} \text{ ou } q' \in p\mathbb{Z}] \text{ (car } p\mathbb{Z} \text{ est un idéal premier de } \mathbb{Z})$$

$$\Rightarrow [p|q \text{ ou } p|q'] \Rightarrow [q = p \text{ ou } q' = p]$$

$$\Rightarrow [q = p \text{ ou } q = 1].$$

Donc  $p$  est un nombre premier.

⇐ ) **Si  $p$  est un nombre premier :**

$$\forall x, y \in \mathbb{Z} \quad tq : xy \in p\mathbb{Z}.$$

$$xy \in p\mathbb{Z} \Rightarrow p|(xy) \Rightarrow [p|x \text{ ou } p|y] \Rightarrow [x \in p\mathbb{Z} \text{ ou } y \in p\mathbb{Z}].$$

Donc  $p\mathbb{Z}$  est un idéal premier de  $\mathbb{Z}$ .

Alors  $p\mathbb{Z}$  est un idéal premier de  $\mathbb{Z}$  si et seulement si  $p$  est un nombre premier.

Ce qui montre que les idéaux premiers de  $\mathbb{Z}$  sont  $\{0\}$ ,  $\mathbb{Z}$  et les idéaux de  $p\mathbb{Z}$  tels  $p$  soit un nombre premier.

6) Soit  $p$  un entier naturel quelconque.

Montrons que  $p\mathbb{Z}$  est un idéal maximal de  $\mathbb{Z}$  si et seulement si  $p$  est un nombre premier.

⇒ ) **Si  $p\mathbb{Z}$  est un idéal maximal de  $\mathbb{Z}$  :**

$$\text{Alors : } p\mathbb{Z} \neq \mathbb{Z} \Rightarrow p \neq 1.$$

Soit  $q$  un diviseur quelconque de  $p$ .

$$q|p \Rightarrow p\mathbb{Z} \subset q\mathbb{Z} \Rightarrow [q\mathbb{Z} = p\mathbb{Z} \text{ ou } q\mathbb{Z} = \mathbb{Z}] \Rightarrow [q = p \text{ ou } q = 1].$$

Donc  $p$  est un nombre premier.

⇐ ) **Si  $p$  est un nombre premier :**

$$\text{Alors : } p \neq 1 \Rightarrow p\mathbb{Z} \neq \mathbb{Z}.$$

Soit  $J$  un idéal de  $\mathbb{Z}$  contenant  $p\mathbb{Z}$ . Il existe un entier naturel  $q$  tel que  $J = q\mathbb{Z}$ .

$$p\mathbb{Z} \subset J = q\mathbb{Z} \Rightarrow q|p \Rightarrow [q = p \text{ ou } q = 1] \Rightarrow [J = p\mathbb{Z} \text{ ou } J = \mathbb{Z}].$$

Donc  $p\mathbb{Z}$  est un idéal maximal de  $\mathbb{Z}$ .

Ce qui montre que les idéaux maximaux de  $\mathbb{Z}$  les idéaux  $p\mathbb{Z}$  tels  $p$  soit un nombre premier.

7) Soit  $B$  un autre anneau et  $f$  est un homomorphisme d'anneaux de  $A$  vers  $B$ .

Soit  $J$  est un idéal premier de  $B$ .

$$\forall x, y \in A \quad tq : xy \in f^{-1}(J).$$

$$xy \in f^{-1}(J) \Rightarrow f(xy) \in J \Rightarrow f(x)f(y) \in J \Rightarrow [f(x) \in J \text{ ou } f(y) \in J]$$

$$\Rightarrow [x \in f^{-1}(J) \text{ ou } y \in f^{-1}(J)].$$

Donc  $f^{-1}(J)$  est un idéal premier de  $A$ .

**Définition 4-5-5 :**

Soit  $A$  un anneau commutatif unitaire intègre.

- \* On dit qu'un idéal  $I$  de  $A$  est principal s'il existe un élément  $a \in A$  tel que  $I = aA$ .
- \* Si les idéaux de  $A$  sont tous principaux, on dit que l'anneau  $A$  est principal.

**Exemple 4-5-6 :**

- \* Les corps sont tous des anneaux principaux.  
Car, si  $A$  est un corps alors les idéaux de  $A$  sont  $\{0_A\} = 0_AA$  et  $A = 1_AA$ .
- \*  $\mathbb{Z}$  est un anneau principal.

**Définition 4-5-7 :**

Soit  $A$  un anneau commutatif unitaire intègre.

On dit que  $A$  est un anneau euclidien s'il existe une application  $f$  de  $A^*$  vers  $\mathbb{N}$  telle que pour tout élément  $a$  de  $A$  et pour tout élément non nul  $b$  de  $A^*$  il existe deux

$$\text{éléments } q \text{ et } r \text{ de } A \text{ tels que : } \begin{cases} a = bq + r \\ r = 0 \text{ ou } (r \neq 0 \text{ et } f(r) < f(b)) \end{cases} .$$

**Exemple 4-5-8 :**

- \* Les corps sont tous des anneaux euclidiens.

**En effet :**

Soient  $A$  un corps et  $f$  l'application de  $A^*$  vers  $\mathbb{N}$  définie par :  $f : A^* \rightarrow \mathbb{N}$   
 $x \mapsto f(x) = 0$ .

$$\forall a \in A \text{ et } \forall b \in A^* : a = b(b^{-1}a) + 0.$$

Donc  $A$  est un anneau euclidien.

- \*  $\mathbb{Z}$  est un anneau euclidien.

**En effet :**

Soit  $f$  l'application de  $\mathbb{Z}^*$  vers  $\mathbb{N}$  définie par :  $f : \mathbb{Z}^* \rightarrow \mathbb{N}$   
 $x \mapsto f(x) = |x|$ .

$$\forall a \in \mathbb{Z} \text{ et } \forall b \in \mathbb{Z}^* : \exists q, r \in \mathbb{Z} \text{ tq : } \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases} .$$

Si  $r \neq 0$  alors  $f(r) = |r| < |b| = f(b)$ .

Donc  $\mathbb{Z}$  est un anneau euclidien.

**Théorème 4-5-9 :**

Les anneaux euclidiens sont principaux.

**Démonstration :**

Soit  $A$  un anneau euclidien et  $f$  une application de  $A^*$  vers  $\mathbb{N}$  telle que pour tout élément  $a$  de  $A$  et pour tout élément non nul  $b$  de  $A^*$  il existe deux éléments  $q$  et  $r$

$$\text{tels que : } \begin{cases} a = bq + r \\ r = 0 \text{ ou } (r \neq 0 \text{ et } f(r) < f(b)) \end{cases} .$$

Soit  $I$  un idéal quelconque de  $A$ .

- **Si  $I$  est nul :**

Alors  $I = \{0_A\} = 0_A A$  est un idéal principal.

- **Si  $I$  n'est pas nul :**

Alors  $I^* = I - \{0_A\}$  n'est pas vide et par suite  $f(I^*)$  n'est pas vide.

Soit  $m$  le plus petit élément de  $f(I^*)$  et soit  $a$  un élément de  $A$  tel que  $f(a) = m$ .

$a \in I^* \subset I \Rightarrow aA \subset I$ .

$$\forall x \in I : \exists q, r \in A \text{ tq : } \begin{cases} x = aq + r \\ r = 0 \text{ ou } (r \neq 0 \text{ et } f(r) < f(a) = m) \end{cases} .$$

$x = aq + r \Rightarrow r = x - aq \in I$  (car  $I$  est un idéal de  $A$  et  $x, a \in I$ ).

Supposons que  $r \neq 0$ . Alors :  $r \in I^* \Rightarrow f(r) \in f(I^*) \Rightarrow f(r) \geq m$ . Ce qui est absurde.

Donc :  $r = 0 \Rightarrow x = aq \in aA$ . Par suite  $I \subset aA$ . Alors  $I = aA$  est un idéal principal.

Ce qui montre que  $A$  est un anneau principal.

#### 4-6-Anneaux quotients :

##### **Théorème et définition 4-6-1 :**

Soient  $A$  un anneau,  $I$  un idéal de  $A$  et  $\pi$  la surjection canonique du groupe additif  $A$  vers le groupe additif  $A/I$ .

1) Il existe une loi de composition interne et une seule dans l'ensemble  $A/I$  noté multiplicativement tel que  $\pi$  soit un homomorphisme de  $(A, .)$  vers  $(A/I, .)$ .

2)  $\forall x, y \in A : \overline{xy} = \overline{x}\overline{y}$ .

3)  $(A/I, +, .)$  est un anneau appelé l'anneau quotient  $A/I$ , et  $\pi$  est un homomorphisme d'anneaux de  $(A, +, .)$  vers  $(A/I, +, .)$ .

4) Si  $A$  est abélien alors  $A/I$  est abélien.

5) Si  $A$  est unitaire alors  $A/I$  est unitaire dont l'unité est  $p(1_A) = \overline{1_A}$ .

##### **Démonstration :**

1) - **Existence :**

Soit  $\varphi$  la relation de  $(A/I) \times (A/I)$  vers  $A/I$  définie par :

$\forall (X, Y) \in (A/I) \times (A/I) \text{ et } \forall Z \in (A/I) :$

$$(X, Y) \varphi Z \Leftrightarrow \exists (x, y, z) \in X \times Y \times Z \text{ tq : } xy = z.$$

Montrons que  $\varphi$  est une loi de composition dans  $A/I$  qui sera notée multiplicativement.

$$\forall (X, Y) \in (A/I) \times (A/I) \text{ et } \forall Z, Z' \in (A/I) \text{ tq : } \begin{cases} (X, Y) \varphi Z \\ (X, Y) \varphi Z' \end{cases} .$$

$$(X, Y) \varphi Z \Rightarrow \exists (x, y, z) \in X \times Y \times Z \text{ tq : } xy = z.$$

$$(X, Y) \varphi Z' \Rightarrow \exists (x', y', z') \in X \times Y \times Z \text{ tq : } x'y' = z'.$$

$$z - z' = xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y').$$

$$\begin{cases} x, x' \in X \Rightarrow x - x' \in I \\ y, y' \in Y \Rightarrow y - y' \in I \end{cases} \Rightarrow z - z' = (x - x')y + x'(y - y') \in I.$$

Par suite :  $Z = \bar{z} = \bar{z}' = Z'$  Donc  $\varphi$  est une fonction de  $(A/I) \times (A/I)$  vers  $A/I$ .

$$\forall (X, Y) \in (A/I) \times (A/I) : \exists (x, y) \in X \times Y \text{ tq : } [X = \bar{x} \text{ et } Y = \bar{y}].$$

Posons  $z = xy$ , on a alors :  $(x, y, z) \in X \times Y \times \bar{z}$  et  $xy = z$ .

Par suite :  $(X, Y)\varphi\bar{z} \Rightarrow (X, Y) \in D_\varphi$ .

Ce qui prouve que  $\varphi$  est une application de  $(A/I) \times (A/I)$  vers  $A/I$ .

Alors  $\varphi$  est une loi de composition interne dans  $A/I$  qui sera notée multiplicativement.

$\forall x, y \in A$  : posons  $xy = z$ . Alors :

$$\begin{cases} x \in \bar{x} = \pi(x) \\ y \in \bar{y} = \pi(y) \\ xy = z \in \bar{z} = \pi(z) = \pi(xy) \end{cases} \Rightarrow (\pi(x), \pi(y))\varphi\pi(xy) \Rightarrow \pi(xy) = \varphi((\pi(x), \pi(y))) = \pi(x)\pi(y).$$

Ce qui montre que  $\pi$  est un homomorphisme de  $(A, .)$  vers  $(A/I, .)$ .

- **Unicité :**

Soit  $\star$  une autre loi de composition interne dans  $A/I$  telle que  $\pi$  soit un homomorphisme de  $(A, .)$  vers  $(A/I, \star)$ .

$$\forall X, Y \in A/I : \exists x, y \in A \text{ tq : } \begin{cases} X = \pi(x) \\ Y = \pi(y) \end{cases} \quad (\text{car } \pi \text{ est surjectif}).$$

$$X \star Y = \pi(x) \star \pi(y) = \pi(xy) = \pi(x)\pi(y) = XY.$$

D'où l'unicité.

$$2) \forall x, y \in A : \bar{xy} = \pi(xy) = \pi(x)\pi(y) = \bar{x}\bar{y}.$$

$$3) \bullet \forall X, Y, Z \in A/I : \exists x, y, z \in A \text{ tq : } \begin{cases} X = \pi(x) \\ Y = \pi(y) \\ Z = \pi(z) \end{cases}.$$

$$(XY)Z = [\pi(x)\pi(y)]\pi(z) = \pi(xy)\pi(z) = \pi((xy)z) = \pi(x(yz)) = \pi(x)\pi(yz) = \pi(x)[\pi(y)\pi(z)] = X(YZ).$$

Donc la multiplication de  $A/I$  est associative.

$$\bullet \forall X, Y, Z \in A/I : \exists x, y, z \in A \text{ tq : } \begin{cases} X = \pi(x) \\ Y = \pi(y) \\ Z = \pi(z) \end{cases}.$$

$$(X + Y)Z = [\pi(x) + \pi(y)]\pi(z) = \pi(x + y)\pi(z) = \pi((x + y)z) = \pi(xy + xz) = \pi(xy) + \pi(xz) = \pi(x)\pi(y) + \pi(x)\pi(z) = XY + XZ.$$

$$Z(X + Y) = \pi(z)[\pi(x) + \pi(y)] = \pi(z)\pi(x + y) = \pi(z(x + y)) = \pi(zx + zy) = \pi(zx) + \pi(zy) = \pi(z)\pi(x)\pi(y) + \pi(z)\pi(y) = ZX + ZY.$$

Donc la multiplication de  $A/I$  est distributive par rapport à l'addition.

Ce qui montre que  $(A/I, +, .)$  est un anneau et que  $\pi$  est un homomorphisme d'anneaux de  $(A, +, .)$  vers  $(A/I, +, .)$ .

4) Si  $A$  est abélien.

$$\forall X, Y \in A/I : \exists x, y \in A \text{ tq : } \begin{cases} X = \pi(x) \\ Y = \pi(y) \end{cases}.$$

$$XY = \pi(x)\pi(y) = \pi(xy) = \pi(yx) = \pi(y)\pi(x) = YX.$$

Donc  $A/I$  est abélien.



5) Si  $A$  est unitaire.

$$\forall X \in A/I : \exists x \in A \text{ tq : } X = \pi(x).$$

$$\begin{cases} X\pi(1_A) = \pi(x)\pi(1_A) = \pi(x1_A) = \pi(x) = X \\ \pi(1_A)X = \pi(1_A)\pi(x) = \pi(1_Ax) = \pi(x) = X \end{cases}$$

Donc  $\pi(1_A) = \overline{1_A}$  est l'unité de  $A/I$ .

#### Exemple 4-6-2 :

Pour tout entier naturel,  $\mathbb{Z}/n\mathbb{Z}$  est un anneau commutatif unitaire.

**Car :**  $\mathbb{Z}$  est un anneau commutatif unitaire.

#### Notation 4-6-3 :

Pour tout entier naturel  $n$  le groupe multiplicatif  $U(\mathbb{Z}/n\mathbb{Z})$  des éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$  est noté  $U_n$ .

#### Proposition 4-6-4 :

Pour tout entier naturel  $n : U_n = \{ \overline{k} \text{ tq : } k \in \mathbb{Z} \text{ et } k \wedge n = 1 \}.$

#### Démonstration :

Soient  $n$  un entier naturel et  $k$  un entier relatif.

$\Rightarrow$  ) Si  $\overline{k} \in U_n$  :

Alors il existe un entier relatif  $u$  tel que  $\overline{u} \overline{k} = \overline{1}$ .

Donc :  $uk - 1 \in n\mathbb{Z} \Rightarrow [\exists v \in \mathbb{Z} \text{ tq : } uk - 1 = vn] \Rightarrow [\exists v \in \mathbb{Z} \text{ tq : } uk - vn = 1].$

Par suite  $k$  et  $n$  sont premiers entre eux.

$\Leftarrow$  ) Si  $k$  et  $n$  sont premiers entre eux :

Alors il existe deux entiers relatifs  $u$  et  $v$  tels que  $uk + vn = 1$ .

Donc :  $uk - 1 = -vn \in n\mathbb{Z} \Rightarrow \overline{u} \overline{k} = \overline{uk} = \overline{1} \Rightarrow \overline{k} \in U_n.$

Ce qui montre que :  $U_n = \{ \overline{k} \text{ tq : } k \in \mathbb{Z} \text{ et } k \wedge n = 1 \}.$

#### Exemple 4-6-5 :

$$\star U_0 = \{ \overline{k} \text{ tq : } k \in \mathbb{Z} \text{ et } k \wedge 0 = 1 \} = \{ \overline{1}, \overline{-1} \} = \{ \overline{1}, -\overline{1} \}.$$

$$\star U_1 = \{ \overline{k} \text{ tq : } k \in \mathbb{Z} \text{ et } k \wedge 1 = 1 \} = \{ \overline{k} \text{ tq : } k \in \mathbb{Z} \} = \mathbb{Z}/\mathbb{Z} = \{ \overline{0} \}.$$

$$\star U_2 = \{ \overline{1} \}, U_3 = \{ \overline{1}, \overline{2} \}, U_4 = \{ \overline{1}, \overline{3} \} \text{ et } U_{15} = \{ \overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14} \}.$$

#### Propriétés 4-6-6 :

Soit  $A$  un anneau,  $I$  un idéal de  $A$  et  $\pi$  la surjection canonique de  $A$  vers  $A/I$ .

1) Si  $J$  est un idéal de  $A$  alors  $(J+I)/I = \pi(J)$  est un idéal de  $A/I$ .

**En particulier :** si  $I \subset J$  alors  $J/I = \pi(J)$  est un idéal de  $A/I$ .

2) Soient  $J$  et  $K$  deux idéaux de  $A$  contenant  $I$ .

i) Si  $J/I \subset K/I$  alors  $J \subset K$ .

ii) Si  $J/I = K/I$  alors  $J = K$ .

3) Si  $K$  est un idéal de  $A/I$  alors  $\pi^{-1}(K)$  est un idéal de  $A$  contenant  $I$ .

4) Si  $K$  est un idéal de  $A/I$  alors  $K = \pi^{-1}(K)/I$ , et  $\pi^{-1}(K)$  est le seul idéal  $J$  de  $A$  contenant  $I$  tel que  $K = J/I$ .

**Démonstration :**

1) Soit  $J$  un idéal de  $A$ .

- $\subset$ )  $\forall x \in (J+I)/I$  :

$$\exists u \in J \quad \text{et} \quad \exists v \in I \quad \text{tq} : x = \overline{u+v}.$$

$$\text{Alors : } x = \overline{u} + \overline{v} = \overline{u} + \overline{0_A} = \overline{u} = \pi(u) \in \pi(J).$$

$$\text{Donc : } (J+I)/I \subset \pi(J).$$

- $\supset$ )  $\forall x \in \pi(J)$  :

$$\exists u \in J \quad \text{tq} : x = \pi(u) = \overline{u}$$

$$u \in J \subset (J+I) \Rightarrow x = \overline{u} \in (J+I)/I.$$

$$\text{Donc : } \pi(J) \subset (J+I)/I.$$

$$\text{Alors } (J+I)/I = \pi(J).$$

- Puisque  $J$  est un idéal de  $A$  et puisque  $\pi$  est un homomorphisme surjectif de  $A$  vers  $A/I$  alors  $(J+I)/I = \pi(J)$  est un idéal de  $A/I$ .

**En particulier :**

Si  $I \subset J$  alors :  $J+I = J \Rightarrow J/I = (J+I)/I = \pi(J)$  est un idéal de  $A/I$ .

2) i) Supposons que  $J/I \subset K/I$ .

$$\forall a \in J : \overline{a} \in J/I \subset K/I \Rightarrow \exists b \in K \quad \text{tq} : \overline{a} = \overline{b}.$$

$$\text{Alors : } a - b \in I \subset K \Rightarrow a \in K \quad (\text{car } a - b \in K \text{ et } b \in K).$$

$$\text{Donc : } J \subset K.$$

ii) Supposons que  $J/I = K/I$  alors  $J = K$ .

$$J/I = K/I \Rightarrow [J/I \subset K/I \text{ et } K/I \subset J/I] \Rightarrow [J \subset K \text{ et } K \subset J] \Rightarrow J = K.$$

3) Soit  $K$  un idéal de  $A/I$ .

- Puisque  $K$  est un idéal de  $A/I$  et puisque  $\pi$  est un homomorphisme de  $A$  vers  $A/I$  alors  $\pi^{-1}(K)$  est un idéal de  $A$ .

$$I = \ker \pi = \pi^{-1}(\{0_{A/I}\}) \subset \pi^{-1}(K).$$

Donc  $\pi^{-1}(K)$  est un idéal de  $A$  contenant  $I$ .

4) Soit  $K$  un idéal de  $A/I$ .

$$K = \pi(\pi^{-1}(K)) = \pi^{-1}(K)/I.$$

- Soit  $J$  un idéal quelconque de  $A$  contenant  $I$  tel que  $K = J/I$ .

$$J/I = K = \pi^{-1}(K)/I \Rightarrow J = \pi^{-1}(K).$$

Alors  $K = \pi^{-1}(K)/I$ , et  $\pi^{-1}(K)$  est le seul idéal  $J$  de  $A$  contenant  $I$  tel que  $K = J/I$ .

**Théorème 4-6-7 :**

Soient  $A$  un anneau et  $I$  un idéal de  $A$ . Pour que  $I$  soit un idéal premier de  $A$  il faut et il suffit que  $A/I$  soit intègre.

**Démonstration :**

$\Rightarrow$ ) Si  $I$  est un idéal premier de  $A$  :

$$\forall x, y \in A/I \quad \text{tq} : xy = \overline{0_A}.$$

$$x, y \in A/I \Rightarrow [\exists a, b \in A \quad \text{tq} : x = \overline{a} \quad \text{et} \quad y = \overline{b}].$$

$$\text{Alors : } \overline{ab} = \overline{a}\overline{b} = xy = \overline{0_A} \Rightarrow ab \in I \Rightarrow [a \in I \text{ ou } b \in I]$$

$$\Rightarrow [x = \overline{a} = \overline{0_A} \text{ ou } y = \overline{b} = \overline{0_A}].$$

Donc  $A/I$  est intègre.

$\Leftarrow$ ) Si  $A/I$  est intègre :

$\forall a, b \in A \quad tq : ab \in I.$

Alors :  $\overline{ab} = \overline{a}\overline{b} = \overline{0_A} \Rightarrow [\overline{a} = \overline{0_A} \text{ ou } \overline{b} = \overline{0_A}]$  (car  $A/I$  est intègre)  
 $\Rightarrow [a \in I \text{ ou } b \in I].$

Donc  $I$  un idéal premier de  $A$ .

**Exemple 4-6-8 :**

1) Si  $p$  est un entier naturel alors  $\mathbb{Z}/p\mathbb{Z}$  est un intègre si seulement si  $p = 0$  ou  $p = 1$  ou  $p$  est un nombre premier.

**Car**, les idéaux premiers de  $\mathbb{Z}$  sont  $\{0\} = 0\mathbb{Z}$ ,  $\mathbb{Z} = 1\mathbb{Z}$  et les idéaux de  $\mathbb{Z}$  tels  $p$  soit un nombre premier.

2)  $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\}$ ,  $\mathbb{Z}/\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/5\mathbb{Z}$  et  $\mathbb{Z}/7\mathbb{Z}$  sont des anneaux intègres.

3)  $\mathbb{Z}/4\mathbb{Z}$ ,  $\mathbb{Z}/6\mathbb{Z}$ ,  $\mathbb{Z}/8\mathbb{Z}$ ,  $\mathbb{Z}/9\mathbb{Z}$ ,  $\mathbb{Z}/10\mathbb{Z}$  et  $\mathbb{Z}/12\mathbb{Z}$  ne sont pas des anneaux intègres.

**Théorème 4-6-9 :**

Soient  $A$  un anneau et  $I$  un idéal de  $A$ . Si  $A/I$  est un corps alors  $I$  est un idéal maximal de  $A$ .

**Démonstration :**

Supposons que  $A/I$  est un corps.

Puisque  $A/I$  est un corps alors  $A/I$  est non nul et par suite  $I \neq A$ .

Soit  $J$  un idéal de  $A$  contenant  $I$ . Alors  $J/I$  est idéal de  $A/I$ .

Par suite  $J/I = \{\overline{0_A}\} = I/I$  ou  $J/I = A/I$  (car  $A/I$  est un corps).

Donc (d'après la propriété 4-6-6-2) ii)  $J = I$  ou  $J = A$ .

Ce qui montre que  $I$  est un idéal maximal de  $A$ .

**Théorème 4-6-10 :**

Soient  $A$  un anneau commutatif unitaire et  $I$  un idéal de  $A$ . Pour que  $I$  soit un idéal maximal de  $A$  il faut et il suffit que  $A/I$  soit un corps.

**Démonstration :**

$\Leftarrow$ ) Si  $A/I$  est un corps :

Alors, d'après le théorème précédent  $I$  est un idéal maximal de  $A$ .

$\Rightarrow$ ) Si  $I$  est un idéal maximal de  $A$  :

Puisque  $I$  est un idéal maximal de  $A$  alors  $I \neq A$ , par suite  $A/I$  est non nul.

$\forall x \in (A/I)^* : \exists a \in A \quad tq : x = \overline{a}. \quad \overline{a} = x \in (A/I)^* \Rightarrow a \notin I.$

$aA$  est un idéal de  $A$  contenant  $a$  (car  $A$  un anneau commutatif unitaire).

Donc : 
$$\left\{ \begin{array}{l} I \subset aA + I \\ I \neq aA + I \text{ (car } a \in I + aA \text{ et } a \notin I) \Rightarrow aA + I = A \Rightarrow 1 \in (aA + I). \\ I \text{ est un idéal maximal de } A \end{array} \right.$$

Alors il existe un élément  $b$  de  $A$  et un élément  $u$  de  $I$  tels que  $ab + u = 1$ .  
 $ab + u = 1 \Rightarrow ab - 1 = u \in I \Rightarrow \overline{ab} = \overline{1} \Rightarrow x\overline{b} = \overline{a}\overline{b} = \overline{ab} = \overline{1} \Rightarrow x \in U(A/I)$ .  
 On a donc montré que  $U(A/I) = (A/I)^*$ , ce qui montre que  $A/I$  est un corps.

#### Exemple 4-6-11 :

1) Si  $p$  est un entier naturel alors  $\mathbb{Z}/p\mathbb{Z}$  est un corps si et seulement si  $p$  est un nombre premier.

**Car**,  $\mathbb{Z}$  est un anneau commutatif unitaire et les idéaux maximaux de  $\mathbb{Z}$  les idéaux de  $\mathbb{Z}$  tels  $p$  soit un nombre premier.

2)  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/5\mathbb{Z}$  et  $\mathbb{Z}/7\mathbb{Z}$  sont des corps.

3)  $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\}$ ,  $\mathbb{Z}/\mathbb{Z}$ ,  $\mathbb{Z}/4\mathbb{Z}$ ,  $\mathbb{Z}/6\mathbb{Z}$ ,  $\mathbb{Z}/8\mathbb{Z}$ ,  $\mathbb{Z}/9\mathbb{Z}$  et  $\mathbb{Z}/10\mathbb{Z}$  ne sont pas des corps.

#### Corollaire 4-6-12 :

Si  $A$  est un anneau commutatif unitaire alors tous les idéaux maximaux de  $A$  sont des idéaux premiers.

#### Démonstration :

Soient  $A$  un anneau commutatif unitaire et  $I$  un idéal maximal de  $A$ .

D'après le théorème précédent  $A/I$  est un corps.

Par suite  $A/I$  est un anneau intègre. Donc  $I$  un idéal premier de  $A$ .

### 4-7- Caractéristique :

#### Définition 4-7-1 :

Soient  $A$  un anneau et  $a \in A$ .

- Si le sous-groupe additif  $\langle a \rangle$  de  $A$  est d'ordre fini  $p$  :  
on dit que  $a$  est de caractéristique  $p$  et on note,  $\text{cara}(a) = p$ .
- Si le sous-groupe additif  $\langle a \rangle$  de  $A$  est d'ordre infini :  
on dit que  $a$  est de caractéristique 0 et on note,  $\text{cara}(a) = 0$ .

#### Exemples et propriétés 4-7-2 :

Soient  $A$  un anneau .

1)  $\text{cara}(0) = 1$ .

2)  $\forall a \in A^* : \text{cara}(a) \neq 1$ .

3) Si  $A = \mathbb{Z}$  alors :  $\forall a \in \mathbb{Z}^* : \text{cara}(a) = 0$ .

4) Si  $n \in \mathbb{N}^*$  et si  $A = \mathbb{Z}/n\mathbb{Z}$  alors :  $\forall k \in \mathbb{Z} : \text{cara}(\overline{k}) = \frac{n}{k \wedge n}$ .

5) Pour tout élément  $a$  de  $A$ , les trois propriétés suivantes sont équivalentes :

- i)  $\text{cara}(a) = 0$ .
- ii)  $\forall k \in \mathbb{Z}^* : ka \neq 0$ .
- iii)  $\forall k \in \mathbb{N}^* : ka \neq 0$ .

6) Pour tout élément  $a$  de  $A$ , les trois propriétés suivantes sont équivalentes :

- i)  $\text{cara}(a) \neq 0$ .
- ii)  $\exists k \in \mathbb{N}^* \quad tq : ka = 0$ .
- iii)  $\exists k \in \mathbb{Z}^* \quad tq : ka = 0$ .

7) Pour tout élément  $a$  de  $A$ .

i) Si  $\text{cara}(a) \neq 0$  alors  $\text{cara}(a)$  est le plus petit entier naturel non nul  $k$  tel que  $ka = 0$ .

ii)  $\forall k \in \mathbb{Z} : ka = 0 \Leftrightarrow \text{cara}(a) | k$ .

### Démonstration :

1)  $\text{cara}(0) = |\langle 0 \rangle| = 1$ .

2)  $\forall a \in A^* :$

– Si  $a$  est d'ordre infini :

Alors :  $\text{cara}(a) = 0 \neq 1$ .

– Si  $a$  est d'ordre fini :

Alors :  $\text{cara}(a) = |a| = |\langle a \rangle| \geq 2$  (car  $a \neq 0$  et  $0, a \in \langle a \rangle$ ).

Donc :  $\text{cara}(a) \neq 1$ .

3) Supposons que  $A = \mathbb{Z}$ .

$\forall a \in \mathbb{Z}^* : \langle a \rangle = |a|\mathbb{Z}$  est d'ordre infini. Donc :  $\text{cara}(a) = 0$ .

4) Supposons que  $n \in \mathbb{N}^*$  et que  $A = \mathbb{Z}/n\mathbb{Z}$ .

$\forall k \in \mathbb{Z} : \text{cara}(\bar{k}) = |\langle \bar{k} \rangle| = |\bar{k}| = \frac{n}{k \wedge n}$ .

5) Soit  $a$  un élément quelconque de  $A$ .

D'après la définition 4-7-1,  $\text{cara}(a) = 0$  si seulement si  $a$  est d'ordre infini.

Ce qui montre (d'après la propriété 7) du théorème 2-4-7), que les trois propriétés i), ii) et iii) sont équivalentes.

6) Soit  $a$  un élément quelconque de  $A$ .

D'après la définition 4-7-1,  $\text{cara}(a) \neq 0$  si seulement si  $a$  est d'ordre fini.

Ce qui montre (d'après la propriété 5) du théorème 2-4-7), que les trois propriétés i), ii) et iii) sont équivalentes.

7) Soit  $a$  un élément quelconque de  $A$ .

i) Supposons que  $\text{cara}(a) \neq 0$ .

Puisque  $|a| = |\langle a \rangle| = \text{cara}(a)$ , alors (d'après la propriété 6) ii) du théorème 2-4-7),  $\text{cara}(a)$  est le plus petit entier naturel non nul  $k$  tel que  $ka = 0$ .

ii)  $\forall k \in \mathbb{Z} :$

– Si  $\text{cara}(a) = 0 :$

D'après 5),  $ka = 0 \Leftrightarrow k = 0 \Leftrightarrow 0 | k \Leftrightarrow \text{cara}(a) | k$ .

– Si  $\text{cara}(a) \neq 0 :$

Alors  $a$  est d'ordre fini et  $\text{cara}(a) = |a|$ .

D'après la propriété 6) ii) du théorème 2-4-7), on a :

$ka = 0 \Leftrightarrow |a| | k \Leftrightarrow \text{cara}(a) | k$ .

### Théorème et définition 4-7-3 :

Si  $A$  est anneau intègre non nul alors tous les éléments non nuls de  $A$  ont la même caractéristique qui est soit 0 soit un nombre premier, appelé la caractéristique de  $A$  et noté  $\text{cara}(A)$ .

**Démonstration :**

Soit  $A$  un anneau intègre non nul.

★ Soient  $a$  et  $b$  deux éléments quelconques non nuls de  $A$ .

Posons  $\text{cara}(a) = p$ ,  $\text{cara}(b) = q$ , et montrons que  $p = q$ .

- **Si  $p = 0$  :**

$$\forall k \in \mathbb{N}^* : ka \neq 0 \Rightarrow (ka)b \neq 0 \Rightarrow a(kb) \neq 0 \Rightarrow kb \neq 0.$$

$$\text{Donc : } \text{cara}(b) = 0 = q \Rightarrow p = 0 = q.$$

- **Si  $p \neq 0$  :**

$$a(pb) = (pa)b = 0b = 0 \Rightarrow pb = 0 \text{ (car } a \neq 0). \text{ Alors } q \neq 0 \text{ et } q|p.$$

$$(qa)b = a(qb) = a0 = 0 \Rightarrow qa = 0 \text{ (car } b \neq 0). p|q.$$

$$\text{Donc : } p = q.$$

★ On a alors montrer que tous les éléments non nuls de  $A$  ont la même caractéristique.

★ Soit  $p$  la caractéristique de  $A$  (c'est à dire  $p$  est caractéristique commune des éléments de  $A$ ).

Montrons que si  $p$  est non nul alors  $p$  est un nombre premier.

Supposons que  $p \neq 0$  et soit  $a$  un élément quelconque non nul de  $A$ .

Soit  $q$  un diviseur quelconque de  $p$ .

Alors il existe un entier naturel  $q'$  tel que  $p = qq'$ .

- **Si  $q'a = 0$  :**

$$\text{Alors : } \begin{cases} q'|p \text{ (car } qq' = p) \\ p|q' \text{ (car } q'a = 0) \end{cases} \Rightarrow q' = p \Rightarrow qp = p \Rightarrow q = 1.$$

- **Si  $q'a \neq 0$  :**

$$\text{Alors } \text{cara}(q'a) = p. \text{ Par suite on a : } q(q'a) = (qq')a = pa = 0 \Rightarrow p|q.$$

$$\text{On a donc : } q|p \text{ (car } qq' = p) \text{ et } p|q, \text{ par suite } q = p.$$

Ce qui montre que  $p$  est un nombre premier.

On a donc montrer que la caractéristique de  $A$  est soit 0 soit un nombre premier.

**Exemples 4-7-4 :**

$$* \text{cara}(\mathbb{Z}) = \text{cara}(\mathbb{Q}) = \text{cara}(\mathbb{R}) = \text{cara}(\mathbb{C}) = 0.$$

$$\text{Car : } \text{cara}(\mathbb{Z}) = \text{cara}(\mathbb{Q}) = \text{cara}(\mathbb{R}) = \text{cara}(\mathbb{C}) = \text{cara}(1) = 0.$$

\* Si  $p$  est un nombre premier alors,  $\text{cara}(\mathbb{Z}/p\mathbb{Z}) = p$ .

**Car :** pour tout nombre premier  $p$  on a :

$$\text{cara}(\mathbb{Z}/p\mathbb{Z}) = \text{cara}(\bar{1} \text{ (modulo } n)) = |\bar{1} \text{ (modulo } n)| = |\mathbb{Z}/p\mathbb{Z}| = p.$$

**Remarque 4-7-5 :**

Si  $A$  est un anneau intègre non nul de caractéristique  $p$  et si  $k$  est un multiple de  $p$  alors :  $\forall x \in A : kx = 0$ .

**En effet :**

Soient  $A$  un anneau intègre non nul de caractéristique  $p$  et  $k$  un multiple de  $p$ .

– **Si  $p = 0$  :**

$$\text{Alors : } k = 0 \Rightarrow \forall x \in A : kx = 0x = 0.$$

– Si  $p \neq 0$  :

$\forall x \in A$  :

- Si  $x = 0$  :

$$kx = k0 = 0.$$

- Si  $x \neq 0$  :

Puisque  $\text{cara}(x) = \text{cara}(A) = p$  et puisque  $k$  est un multiple de  $p$  alors (d'après la propriété 4-7-2-7 ii)),  $kx = 0$ .

**Lemme 4-7-6 :**

Si  $p$  est un nombre premier alors pour tout entier naturel  $k = 1, \dots, p-1$ ,  $C_p^k$  est un multiple de  $p$ .

**Démonstration :**

Soient  $p$  un nombre premier et  $k = \{1, \dots, p-1\}$ .

$$C_p^k = \frac{p!}{k!(p-k)!} \Rightarrow p! = k!(p-k)!C_p^k \Rightarrow p \mid [k!(p-k)!C_p^k].$$

Puisque  $p$  est premier avec  $k!(p-k)!$  (car  $p$  est premier avec  $k!$  et  $(p-k)!$ ) et puisque  $p$  est un diviseur de  $k!(p-k)!C_p^k$  alors  $p$  est un diviseur de  $C_p^k$ .

**Théorème 4-7-7 :**

Soient  $A$  un anneau intègre non nul de caractéristique  $p \neq 0$  et  $a, b \in A$ .

Si  $ab = ba$  alors :  $(a+b)^p = a^p + b^p$ .

**Démonstration :**

On suppose que  $ab = ba$ .

$$(a+b)^p = \sum_{k=0}^p C_p^k a^{p-k} b^k = a^p + \sum_{k=1}^{p-1} C_p^k a^{p-k} b^k + b^p = a^p + b^p.$$

D'après le lemme précédent et la remarque précédente on a :

$$\forall k = 1, \dots, p-1 : C_p^k a^{p-k} b^k = 0.$$

On a donc :  $(a+b)^p = a^p + b^p$ .

**Corollaire 4-7-8 :**

Soient  $A$  un anneau intègre non nul de caractéristique  $p \neq 0$  et  $a, b \in A$ .

Si  $ab = ba$  alors :  $\forall n \in \mathbb{N} : (a+b)^{p^n} = a^{p^n} + b^{p^n}$ .

**Démonstration :**

On suppose que  $ab = ba$ .

Montrons par récurrence que pour tout entier naturel  $n$  on a :  $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ .

- Pour  $n = 0$  :

$$(a+b)^{p^0} = (a+b)^{p^0} = (a+b)^1 = a+b = a^1 + b^1 = a^{p^0} + b^{p^0} = a^{p^0} + b^{p^0}.$$

- Pour  $n = 1$  :

$$\text{Supposons que } (a+b)^{p^{n-1}} = a^{p^{n-1}} + b^{p^{n-1}}.$$

- **Pour n :**

Montrons qu'alors :  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ .

$$\begin{aligned}(a + b)^{p^n} &= (a + b)^{p^{n-1}+1} = (a + b)^{p^{n-1}p} = \left[ (a + b)^{p^{n-1}} \right]^p = \left[ a^{p^{n-1}} + b^{p^{n-1}} \right]^p \\ &= \left( a^{p^{n-1}} \right)^p + \left( b^{p^{n-1}} \right)^p = a^{p^{n-1}p} + b^{p^{n-1}p} = a^{p^n} + b^{p^n}.\end{aligned}$$

**Corollaire 4-7-9 :**

Si  $A$  est un anneau commutatif intègre non nul de caractéristique  $p \neq 0$  alors pour tout entier naturel  $n \in \mathbb{N}$  l'application suivante :

$$\begin{aligned}f_n : A &\rightarrow A \\ a &\mapsto f_n(a) = a^{p^n}\end{aligned}$$

est un homomorphisme d'anneaux de  $A$  vers  $A$  qui est unitaire si  $A$  est unitaires.

**Démonstration :**

Soient  $A$  un anneau commutatif intègre non nul de caractéristique  $p \neq 0$ ,  $n$  un entier naturel et  $f_n$  l'application de  $A$  vers  $A$  lui même définie par :

$$\begin{aligned}f_n : A &\rightarrow A \\ a &\mapsto f_n(a) = a^{p^n}.\end{aligned}$$

$$\forall a, b \in A : \begin{cases} f_n(a + b) = (a + b)^{p^n} = a^{p^n} + b^{p^n} = f_n(a) + f_n(b) \\ f_n(ab) = (ab)^{p^n} = a^{p^n} b^{p^n} = f_n(a) f_n(b) \end{cases}.$$

Donc l'application  $f_n$  est un homomorphisme d'anneaux de  $A$  vers  $A$  lui même.

Si du plus  $A$  est unitaire alors :  $f_n(1_A) = (1_A)^{p^n} = 1_A$ .

Dans ce cas  $f_n$  est un homomorphisme d'anneaux unitaires.

**Proposition et notation 4-7-10 :**

Soient  $A$  un anneau commutatif unitaire intègre non nul de caractéristique 0.

★  $\forall n \in \mathbb{Z}^* : n1_A \neq 0$ .

★ Pour tout entier relatif  $n$ , on confond  $n1_A$  avec  $n$ . C'est à dire  $n$  devient un élément de  $A$ .

★  $\mathbb{Z}$  devient un sous-anneau unitaire de  $A$ .